

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-164550

(43)Date of publication of application : 19.06.1998

(51)Int.Cl.

H04N 7/167

H04H 1/00

H04L 9/08

(21)Application number : 08-324209

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 04.12.1996

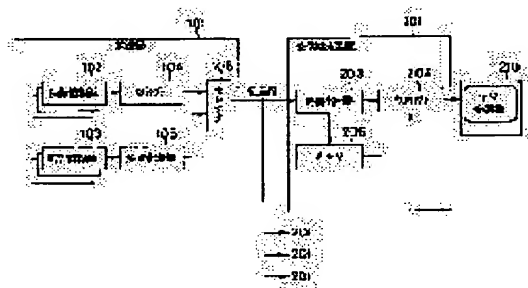
(72)Inventor : YOSHIDA OSAMU

(54) SCRAMBLE SYSTEM, BROADCASTING STATION DEVICE AND RECEIVING TERMINAL DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To positively promote the joining of a sponsor by ensuring the viewing of advertizing information inserted to a program, so as to improve an advertizing effect.

SOLUTION: A broadcasting station 101 gives scrambles to video information (program) selected from video information source 102 by a scrambler 104, multiplexes a key for descrambling advertizing information selected by advertizing information source 103 by a multiplexer 105 and sends video information and advertizing information by arbitrarily switching with a selector receiving terminal devices 201 respectively extract a key for descrambling a key extraction circuit 203 from the advertizing period of the program to store into a memory 206. Then through the use of this key, a descrambler 204 descrambles the program.



LEGAL STATUS

[Date of request for examination] 21.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3585679

[Date of registration] 13.08.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 0 - 1 6 4 5 5 0

(43) 公開日 平成 1 0 年 (1 9 9 8) 6 月 1 9 日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H04N 7/167			H04N 7/167	Z
H04H 1/00			H04H 1/00	F
H04L 9/08			H04L 9/00	601 Z

審査請求 未請求 請求項の数 1 6 O L (全 4 3 頁)

(21) 出願番号 特願平 8 - 3 2 4 2 0 9

(22) 出願日 平成 8 年 (1 9 9 6) 1 2 月 4 日

(71) 出願人 0 0 0 0 0 3 0 7 8
株式会社東芝
神奈川県川崎市幸区堀川町 7 2 番地

(72) 発明者 吉田 治
神奈川県横浜市磯子区新杉田町 8 番地 株
式会社東芝マルチメディア技術研究所内

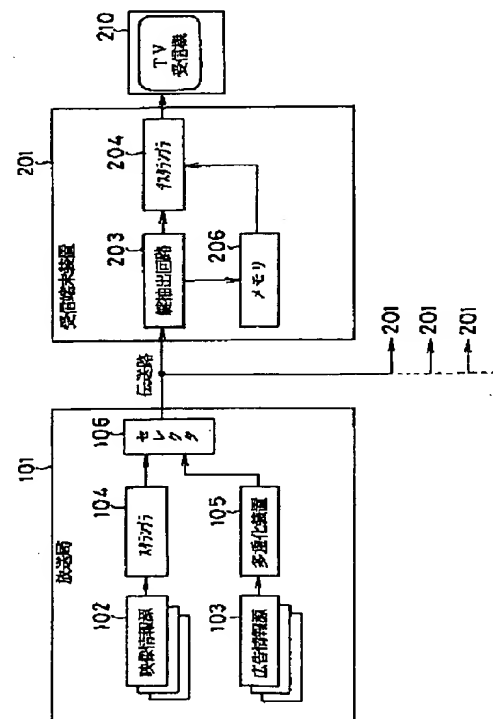
(74) 代理人 弁理士 三好 秀和 (外 3 名)

(54) 【発明の名称】 スクランブル方式および放送局装置および受信端末装置

(57) 【要約】

【課題】 番組中に挿入された広告情報の視聴を保証して広告効果を上げ、積極的にスポンサーの参入を促進する。

【解決手段】 放送局 1 0 1 は、映像情報源 1 0 2 から選ばれた映像情報 (番組) にスクランブラ 1 0 4 によりスクランブルを施し、広告情報源 1 0 3 から選ばれた広告情報にスクランブルを解除する鍵を多重化装置 1 0 5 により多重化し、映像情報と広告情報とをセレクタ 1 0 6 により任意に切り替えて送出する。受信端末装置 2 0 1 は、それぞれ、番組の広告期間中から鍵抽出回路 2 0 3 によりデスクランブルのための鍵を抽出し、メモリ 2 0 6 に記憶する。そして、この鍵を使用してデスクランブラ 2 0 4 が番組のスクランブルを解除する。



【特許請求の範囲】

【請求項 1】 放送または記憶媒体を介して提供される映像にスクランブルを施すスクランブル方式において、前記映像にスクランブルを施すとともに、前記スクランブルを解除するための鍵を多重化した広告情報を前記映像に前置または挿入して提供し、前記映像の再生時に、前記広告情報に多重化された鍵を抽出し、この鍵を用いて前記映像のスクランブルを解除することを特徴とするスクランブル方式。

【請求項 2】 テレビジョン放送の受信を制限するスクランブル方式において、放送局側からは、テレビジョン番組の映像または音声にスクランブルを施すとともに、前記スクランブルを解除するための鍵を多重化した広告情報を前記テレビジョン番組中に挿入して放送し、受信側では、前記テレビジョン番組に挿入された広告情報を受信し、この広告情報に多重化された前記鍵を抽出し、この鍵を用いて前記テレビジョン番組のスクランブルを解除することを特徴とするスクランブル方式。

【請求項 3】 1つのテレビジョン番組中に複数回の広告情報の挿入を行う際に、広告情報の挿入毎にスクランブルを解除するための鍵を変更することを特徴とする請求項 2 に記載のスクランブル方式。

【請求項 4】 テレビジョン番組の映像または音声に任意にスクランブルを施すスクランブル手段と、任意の広告情報を選択する選択手段と、前記スクランブルを解除する鍵を前記選択された広告情報に多重化する多重化手段と、前記スクランブルが施された番組と前記鍵が多重化された広告情報とを任意のタイミング及び頻度で切り替える切替手段と、を備えたことを特徴とする放送局装置。

【請求項 5】 任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、この受信されたテレビジョン放送に挿入された広告情報に多重化された鍵を抽出する抽出手段と、この抽出手段により抽出された鍵を保持する保持手段と、前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、を備えたことを特徴とする受信端末装置。

【請求項 6】 映像または音声にスクランブルが施された番組を第 1 のチャンネルで放送するとともに、前記スクランブルを解除する鍵を広告情報に多重化して第 2 のチャンネルで放送するスクランブル方式であって、前記第 1 のチャンネルでは、前記スクランブルが施された番組に前記第 2 のチャンネルを通知する制御情報を多重化して放送し、前記第 2 のチャンネルでは、前記スクランブルを解除す

る鍵を前記広告情報に多重化して放送し、

受信側では、前記制御情報を参照して、前記スクランブルを解除する鍵を入手し、前記番組のスクランブルを解除することを特徴とするスクランブル方式。

【請求項 7】 テレビジョン番組に任意にスクランブルを施すスクランブル手段と、前記スクランブルが施されたテレビジョン番組に第 2 のチャンネルを通知する制御情報を多重化する第 1 の多重化手段と、前記制御情報が多重化された番組を第 1 のチャンネルに変調する第 1 の変調手段と、広告情報を記憶する記憶手段と、前記記憶手段から所望の広告情報を選択的に読み出す読出手段と、前記スクランブルされたテレビジョン番組のスクランブルを解除する鍵を前記読み出された広告情報に多重化する第 2 の多重化手段と、前記鍵が多重化された広告情報を第 2 のチャンネルに変調する第 2 の変調手段と、を備えたことを特徴とする放送局装置。

【請求項 8】 任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、この受信されたテレビジョン信号に多重化された鍵および第 2 のチャンネルを通知する制御情報を抽出する抽出手段と、この抽出手段により抽出された鍵および制御情報を保持する保持手段と、前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、上記各手段を制御する制御手段と、を備えて成り、前記制御手段は、第 1 のチャンネルで放送されるテレビジョン番組のスクランブルを解除する鍵を入手するために第 2 のチャンネルを受信する必要があるときには、前記抽出された制御情報に基づいて第 2 のチャンネルを受信して前記鍵を抽出するように制御することを特徴とする受信端末装置。

【請求項 9】 前記制御手段は、次に有効な鍵が抽出されるまで、前記保持手段に前記鍵の保持を継続させるとともに、第 1 のチャンネルから第 3 のチャンネルへ受信チャンネルを切り替えた後、再度第 1 のチャンネルを受信チャンネルが復帰されたとき、前記鍵の有効性を検証し、有効であればそのままスクランブル解除に使用し、有効でなければ、再度第 2 のチャンネルを受信して前記鍵を抽出するように制御することを特徴とする請求項 8 に記載の受信端末装置。

【請求項 10】 前記制御回路は、受信した第 1 のチャンネルのスクランブルを解除する有効な鍵がメモリに保存されていないとき、前記受信手段に第 2 のチャンネル

10

20

30

40

50

を受信させ、この第2のチャンネルの広告情報に多重化された鍵を抽出手段に抽出させ、メモリに記憶させた後、第1のチャンネルを受信するように受信手段を制御し、デスクランブラにスクランブルを解除させることを特徴とする請求項8または請求項9に記載の受信端末装置。

【請求項11】 スクランブルが施された有料番組を受信した場合、広告情報を視聴することにより視聴料金を割引または無料化することを表示させる表示制御手段と、

視聴者が広告情報を視聴するかしないかの選択結果を入力する入力手段と、

前記入力された選択結果に基づいて課金処理を行う課金制御手段と、

をさらに備えたことを特徴とする請求項8ないし請求項10のいずれか1項に記載の受信端末装置。

【請求項12】 テレビジョン放送の受信を制限するスクランブル方式において、

放送局側からは、テレビジョン番組の映像または音声に任意にスクランブルを施すとともに、前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを含む情報をこのテレビジョン番組に多重化して放送し、

受信側では、前記テレビジョン番組を受信し、前記テレビジョン番組に多重化された広告情報を構成するためのデータに基づいて、広告情報を構成して表示するとともに、多重化された前記鍵を抽出し、この鍵を用いて前記テレビジョン番組のスクランブルを解除することを特徴とするスクランブル方式。

【請求項13】 テレビジョン番組の映像または音声に任意にスクランブルを施すスクランブル手段と、

広告情報を構成するためのデータを記憶する記憶手段と、

前記記憶手段から所望の広告情報を構成するデータを選択的に読み出す読出手段と、

前記スクランブルを施されたテレビジョン番組に前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを含む情報を多重化する多重化手段と、

前記多重化されたテレビジョン番組を変調する変調手段と、

を備えたことを特徴とする放送局装置。

【請求項14】 任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、

この受信されたテレビジョン放送に多重化された前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを抽出する抽出手段と、

この抽出手段により抽出された鍵および広告情報を構成するためのデータを保持する保持手段と、

前記広告情報を構成するためのデータに基づいて、広告情報を構成して表示させる表示制御手段と、

前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、

を備えたことを特徴とする受信端末装置。

【請求項15】 前記テレビジョン番組は、視聴者からの要求に応じて放送されるオンデマンド方式の番組であり、スクランブルを解除する有効な鍵が保持されていない場合、テレビジョン番組の配信を一時停止し、広告情報を受信するか、或いは料金を払って受信するかを選択を視聴者に提供し、前者が選択された場合、広告情報を放送し、後者が選択された場合、テレビジョン番組を放送して課金を行うことを特徴とする請求項2に記載のスクランブル方式。

【請求項16】 前記スクランブルは、前記テレビジョン番組に対して擬似乱数系列を加算する暗号化及び又はブロック暗号化を行うスクランブルであり、この擬似乱数系列の初期値及び又はブロック暗号の鍵を第1の鍵とし、この第1の鍵より更新周期の長い第2の鍵で第1の鍵と前記番組を識別する情報を暗号化して第1の暗号化データを生成し、各受信端末装置毎に異なる第3の鍵で第2の鍵および対応する受信端末装置に関する情報を暗号化して第2の暗号化データを生成し、第1の暗号化データを前記テレビジョン番組に多重化し、第2の暗号化データを前記広告情報に多重化することを特徴とする請求項2または請求項3または請求項6または請求項12に記載のスクランブル方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、映像情報を地上波放送、衛星放送、CATV（ケーブルテレビジョン）などの放送メディアでの提供やLD（レーザーディスク）、CD-ROM、DVD（デジタルビデオディスク）、ビデオカセットなどのパッケージメディアでの提供において、広告情報を付加することで番組を安価に提供するスクランブル方式に関する。

【0002】

【従来の技術】近年、放送設備（ハードウェア）の提供者と放送内容（ソフトウェア）の提供者とを分離可能とする受託・委託放送制度と、MPEG2に代表されるデジタル圧縮技術の進展により、TV放送の多チャンネル化の動きが活発化してきており、放送衛星や通信衛星を使ったアナログTV放送に加えて、通信衛星を使ったデジタルTVの多チャンネル放送が実現してきている。

【0003】また、CATVにおいても地上波の届かない地域への再放送というものから、ビデオオンデマンド、TVショッピングといった双方向性を生かしたサービスや多チャンネル化で視聴者へサービスを拡充し、1つのメディアとして地位を確立してきている。

【0004】一方、地上波放送ではNHKと民間放送と

いう従来からの形態は変わらず、現在でも主たる放送形態としてその地位を守っている。

【0005】ここでこれら様々なメディアにおける放送内容と課金について目を向けてみる。周知のように地上波放送については、NHKは受信機を設置し受信契約をした視聴者から放送受信料を徴収しているが、民間放送は番組中に挿入した広告による収入で成り立っているため視聴者に対しては課金を行っていない。

【0006】これに対し、BS放送ではNHKは放送受信料、WOWOWは加入料と月々の使用料を視聴者から徴収しており、CS放送も基本的には視聴者から料金を徴収する有料放送である。CATVは地上波の再送＋有料放送という形態であり、数段階に設定された加入料金、チャンネル単位（ペイ・パー・チャンネル）または番組単位（ペイ・パー・ビュー）の視聴料金を視聴者から徴収する仕組みになっている。

【0007】NHKを除いた有料放送は、契約者のみに視聴可能とするため、番組には通常スクランブルが施される。料金支払の契約を行った視聴者は、放送局からデスクランブルするための鍵を受け取り、この鍵を使ってスクランブルされた番組をデスクランブルして視聴する。

【0008】このように、地上波の民間放送以外は基本的に有料放送であり、視聴料金はチャンネル単位やペイ・パー・ビューの様に1つの番組の視聴に関して設定された料金が課金されるのが一般的であり、視聴可能な全てのチャンネルや番組を視聴しようとする視聴料金は大きく膨らんでいくことになる。

【0009】そのため、現在の地上波放送における民間放送のようにCMが入っても料金を安くしてほしいという要求も存在し、このような本来有料放送として提供する番組をCMを挿入することで料金を安くすることが考えられる。

【0010】しかしながら、視聴者はCMが見たいのではなく、料金の低下を望むだけであるので、単純に番組中にCMを挿入しても、CMの期間は他のチャンネルに切り換えるなどしてCMを見ない場合が多いと考えられる。

【0011】このため、視聴者がCMを視聴し広告効果が保証されないと、このようなサービスのスポンサーは獲得できず、このサービス自体の実現が困難になるという問題点がある。

【0012】

【発明が解決しようとする課題】以上の問題点に鑑み、本発明の目的は、有料番組にCMを挿入することにより低価格で番組を提供する場合、視聴者のCM視聴を保証して広告効果を上げ、積極的にスポンサーの参入を促進することである。

【0013】

【課題を解決するための手段】上記目的を達成するた

め、本発明は次の構成を有する。

【0014】すなわち、請求項1記載の発明は、放送または記憶媒体を介して提供される映像にスクランブルを施すスクランブル方式において、前記映像にスクランブルを施すとともに、前記スクランブルを解除するための鍵を多重化した広告情報を前記映像に前置または挿入して提供し、前記映像の再生時に、前記広告情報に多重化された鍵を抽出し、この鍵を用いて前記映像のスクランブルを解除することを要旨とする。

10 【0015】また、請求項2記載の発明は、テレビジョン放送の受信を制限するスクランブル方式において、放送局側からは、テレビジョン番組の映像または音声にスクランブルを施すとともに、前記スクランブルを解除するための鍵を多重化した広告情報を前記テレビジョン番組中に挿入して放送し、受信側では、前記テレビジョン番組に挿入された広告情報を受信し、この広告情報に多重化された前記鍵を抽出し、この鍵を用いて前記テレビジョン番組のスクランブルを解除することを要旨とする。

20 【0016】また、請求項3記載の発明は、請求項2に記載のスクランブル方式において、1つのテレビジョン番組中に複数回の広告情報の挿入を行う際に、広告情報の挿入毎にスクランブルを解除するための鍵を変更することを要旨とする。

【0017】また、請求項4記載の発明は、テレビジョン番組の映像または音声に任意にスクランブルを施すスクランブル手段と、任意の広告情報を選択する選択手段と、前記スクランブルを解除する鍵を前記選択された広告情報に多重化する多重化手段と、前記スクランブルが施された番組と前記鍵が多重化された広告情報とを任意のタイミング及び頻度で切り替える切替手段と、を備えたことを特徴とする放送局装置である。

30 【0018】また、請求項5記載の発明は、任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、この受信されたテレビジョン放送に挿入された広告情報に多重化された鍵を抽出する抽出手段と、この抽出手段により抽出された鍵を保持する保持手段と、前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、を備えたことを要旨とする受信端末装置である。

40 【0019】また、請求項6記載の発明は、映像または音声にスクランブルが施された番組を第1のチャンネルで放送するとともに、前記スクランブルを解除する鍵を広告情報に多重化して第2のチャンネルで放送するスクランブル方式であって、前記第1のチャンネルでは、前記スクランブルが施された番組に前記第2のチャンネルを通知する制御情報を多重化して放送し、前記第2のチャンネルでは、前記スクランブルを解除する鍵を前記広告情報に多重化して放送し、受信側では、前記制御情報を参照して、前記スクランブルを解除する鍵を入手し、

前記番組のスクランブルを解除することを要旨とする。

【0020】また、請求項7記載の発明は、テレビジョン番組の映像または音声に任意にスクランブルを施すスクランブル手段と、前記スクランブルが施されたテレビジョン番組に第2のチャンネルを通知する制御情報を多重化する第1の多重化手段と、前記制御情報が多重化された番組を第1のチャンネルに変調する第1の変調手段と、広告情報を記憶する記憶手段と、前記記憶手段から所望の広告情報を選択的に読み出す読出手段と、前記スクランブルされたテレビジョン番組のスクランブルを解除する鍵を前記読み出された広告情報に多重化する第2の多重化手段と、前記鍵が多重化された広告情報を第2のチャンネルに変調する第2の変調手段と、を備えたことを要旨とする放送局装置である。

【0021】また請求項8記載の発明は、任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、この受信されたテレビジョン信号に多重化された鍵および第2のチャンネルを通知する制御情報を抽出する抽出手段と、この抽出手段により抽出された鍵および制御情報を保持する保持手段と、前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、上記各手段を制御する制御手段と、を備えて成り、前記制御手段は、第1のチャンネルで放送されるテレビジョン番組のスクランブルを解除する鍵を入手するために第2のチャンネルを受信する必要があるときには、前記抽出された制御情報に基づいて第2のチャンネルを受信して前記鍵を抽出するように制御することを要旨とする受信端末装置である。

【0022】また、請求項9記載の発明は、請求項8に記載の受信端末装置において、前記制御手段は、次に有効な鍵が抽出されるまで、前記保持手段に前記鍵の保持を継続させるとともに、第1のチャンネルから第3のチャンネルへ受信チャンネルを切り替えた後、再度第1のチャンネルに受信チャンネルが復帰されたとき、前記鍵の有効性を検証し、有効であればそのままスクランブル解除に使用し、有効でなければ、再度第2のチャンネルを受信して前記鍵を抽出するように制御することを要旨とする。

【0023】また、請求項10記載の発明は、請求項8または請求項9に記載の受信端末装置において、前記制御回路は、受信した第1のチャンネルのスクランブルを解除する有効な鍵がメモリに保存されていないとき、前記受信手段に第2のチャンネルを受信させ、この第2のチャンネルの広告情報に多重化された鍵を抽出手段に抽出させ、メモリに記憶させた後、第1のチャンネルを受信するように受信手段を制御し、デスクランブルにスクランブルを解除させることを要旨とする。

【0024】また、請求項11記載の発明は、請求項8ないし請求項10のいずれか1項に記載の受信端末装置において、スクランブルが施された有料番組を受信した

場合、広告情報を視聴することにより視聴料金を割引または無料化することを表示させる表示制御手段と、視聴者が広告情報を視聴するかしないかの選択結果を入力する入力手段と、前記入力された選択結果に基づいて課金処理を行う課金制御手段と、をさらに備えたことを要旨とする受信端末装置である。

【0025】また、請求項12記載の発明は、テレビジョン放送の受信を制限するスクランブル方式において、放送局側からは、テレビジョン番組の映像または音声に任意にスクランブルを施すとともに、前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを含む情報をこのテレビジョン番組に多重化して放送し、受信側では、前記テレビジョン番組を受信し、前記テレビジョン番組に多重化された広告情報を構成するためのデータに基づいて、広告情報を構成して表示するとともに、多重化された前記鍵を抽出し、この鍵を用いて前記テレビジョン番組のスクランブルを解除することを要旨とする。

【0026】また、請求項13記載の発明は、テレビジョン番組の映像または音声に任意にスクランブルを施すスクランブル手段と、広告情報を構成するためのデータを記憶する記憶手段と、前記記憶手段から所望の広告情報を構成するデータを選択的に読み出す読出手段と、前記スクランブルを施されたテレビジョン番組に前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを含む情報を多重化する多重化手段と、前記多重化されたテレビジョン番組を変調する変調手段と、を備えたことを要旨とする放送局装置である。

【0027】また、請求項14記載の発明は、任意のテレビジョン放送のチャンネルを選択して受信する受信手段と、この受信されたテレビジョン放送に多重化された前記スクランブルを解除するための鍵及び広告情報を構成するためのデータを抽出する抽出手段と、この抽出手段により抽出された鍵および広告情報を構成するためのデータを保持する保持手段と、前記広告情報を構成するためのデータに基づいて、広告情報を構成して表示させる表示制御手段と、前記保持された鍵によりスクランブルされたテレビジョン放送のスクランブルを解除するデスクランブル手段と、を備えたことを要旨とする受信端末装置である。

【0028】また、請求項15記載の発明は、請求項2に記載のスクランブル方式において、前記テレビジョン番組は、視聴者からの要求に応じて放送されるオンデマンド方式の番組であり、スクランブルを解除する有効な鍵が保持されていない場合、テレビジョン番組の配信を一時停止し、広告情報を受信するか、或いは料金を払って受信するかを選択を視聴者に提供し、前者が選択された場合、広告情報を放送し、後者が選択された場合、テレビジョン番組を放送して課金を行うことを要旨とする。

【0029】また、請求項16記載の発明は、請求項2または請求項3または請求項6または請求項12に記載のスクランブル方式において、前記スクランブルは、前記テレビジョン番組に対して擬似乱数系列を加算する暗号化及び又はブロック暗号化を行うスクランブルであり、この擬似乱数系列の初期値及び又はブロック暗号の鍵を第1の鍵とし、この第1の鍵より更新周期の長い第2の鍵で第1の鍵と前記番組を識別する情報を暗号化して第1の暗号化データを生成し、各受信端末装置毎に異なる第3の鍵で第2の鍵および対応する受信端末装置に関する情報を暗号化して第2の暗号化データを生成し、第1の暗号化データを前記テレビジョン番組に多重化し、第2の暗号化データを前記広告情報に多重化することを要旨とする。

【0030】上記構成による本発明においては、放送局側ではTV番組の映像や音声をスクランブルし、これをデスクランブルするための鍵を含む情報をCMの期間に多重し、TV番組と同一のチャンネルや異なるチャンネルで放送し、受信側ではCM期間に多重されたデスクランブル情報を抽出して受信したTV番組の映像や音声をデスクランブルする。

【0031】【作用】本発明においては、映像ソフトウェアの費用の一部（または全部）を広告主（スポンサー）に提供してもらう代わりに、映像ソフトウェアに広告情報（以下、CMとも略す）を挿入するとともに、このCMにスクランブルを解除する鍵を多重化する。そして、視聴者または映像パッケージソフトウェアの購入者は、料金が安く（または無料）になる代わりにCMを視聴することによりスクランブルを解除する鍵を入手する。

【0032】これにより、CMの視聴が保証され、積極的なスポンサーの参加が見込まれるので、有料放送または映像パッケージソフトウェアの低価格化が達成される。

【0033】

【発明の実施の形態】次に、図面を参照して本発明の実施の形態を詳細に説明する。有料番組は料金を支払う視聴者のみに視聴可能とするため、番組には通常スクランブルが施される。料金を支払った（或いは、支払うことを約束した）視聴者は放送局からデスクランブルするための鍵を受け取り、これを使ってスクランブルされた番組をデスクランブルして視聴する。本発明はCMを挿入することで番組の費用をCMのスポンサーに一部（またはすべて）提供してもらい、視聴者の料金負担を軽減するシステムである。つまり、視聴者は料金を支払う（料金を安くする）代わりにCMを視聴することでデスクランブルの鍵を受け取ることが本発明の要点である。

【0034】図1は、本発明の原理をテレビジョン放送を例にして説明する原理説明図である。同図において、映像ソフトウェアの提供者である放送局101は、映像

情報源102と、広告情報源103と、映像情報にスクランブルを施すスクランブラ104と、広告情報に鍵を多重化する多重化装置105と、映像情報と広告情報とを切り替えるセレクト106とを備えている。

【0035】複数の受信端末装置201は、それぞれ、鍵抽出回路203と、スクランブルを解除するデスクランブラ204と、鍵を記憶するためのメモリ206とを備えていて、デスクランブラ204の出力は、テレビジョン受信機210に接続されている。

【0036】また、放送局101と複数の受信端末装置201とを接続する伝送路は、有線、無線を問わない。すなわちCATV、地上波放送または衛星放送のいずれの伝送路でもよい。

【0037】図1において、放送局101は、VTRやテレビカメラからの生映像等の複数の映像情報源102から選択された番組の映像信号及び音声信号にスクランブラ104によりスクランブルを施す。また複数の広告情報源103から番組を提供するスポンサーのCMを選択し、このCMにスクランブルを解除する鍵を多重化装置105により多重化し、セレクト106により番組の前または番組中に鍵が多重化されたCMを挿入して放送する。

【0038】受信端末装置201は、放送を受信し、このCM期間中に多重化されたスクランブルを解除する鍵を鍵抽出回路203により抽出し、メモリ206に記憶する。そして、デスクランブラ204は、この記憶された鍵を使用してスクランブルされた番組のスクランブルを解除し、TV受信機210へ出力する。

【0039】このようにCM期間中デスクランブル鍵が多重化されているので、視聴者はスクランブルされた番組を見ようとすれば、CM期間中も他チャンネルへ切り替えることはできず、このチャンネルを継続しなければならない。これにより、CMの視聴が保証されることになる。

【0040】図2は本発明の第1の実施形態を説明するための放送局側の概念的な構成図である。同図において、放送局101は、VTRやテレビカメラからの生映像等の複数の映像情報源102と、スポンサー毎の広告情報源103と、映像信号及び音声信号にスクランブルを施すスクランブラ104と、広告情報の映像信号にスクランブルを解除する鍵および後述される制御コードを多重化する多重化装置105と、番組と広告情報とを切り替えるセレクト106と、セレクトの出力により所定の搬送波を変調して放送波を発生させる変調器109と、多重化装置における多重化およびセレクト106における切替のタイミングを発生するタイミング発生回路108と、放送局を構成するこれらの装置を制御する管理装置107とを備えている。

【0041】放送局101では管理装置107からの選択信号により複数の映像情報源102のうち適切な情報

10

20

30

40

50

が選択されて1つの番組が構成される。この番組が有料番組として提供される場合は通常管理装置107に制御によりスクランブラ104で映像信号、音声信号ともにスクランブルが施されてセクタ106に出力される。

【0042】ここで、この番組がCM挿入により安く提供される有料番組である場合は、複数の広告情報源103からその番組で使用される番組スポンサーのCMを選択して多重化装置105に出力する。多重化装置105では上記有料番組のスクランブルを解くための鍵と制御データをCMの映像信号のブランキング期間に多重化し、セクタ106に出力する。この多重化方法には、例えば、文字多重放送やキャプションの形式を利用して

もよい。
【0043】ここで多重化するデータは、例えば図25に示す5つのフィールドから構成されていて、パースト的に発生するデータの同期をとるための同期コード、次に続くデータの属性を示す制御コード、CH関連情報、鍵データ、及び誤り検出用のパリティ等の各フィールドで構成される。なお、制御コードの詳細は図32に示す。例えば、制御コード＝“00000001”の場合

は鍵が多重されていることを示す。
【0044】タイミング発生回路108は管理装置107の制御のもとに多重化装置105の多重化タイミングとセクタ106の切り替えタイミングを生成し、各々に供給する。セクタ106で所定の割合で1つの番組に対してCMが挿入されて、変調器109を介して所定のTVチャンネルに変調されて放送される。この管理装置の制御フローチャートを図16に示す。

【0045】図16によれば、まず、管理装置107の選択指示により映像情報源102から番組が選択される（ステップS101）。次いで、この番組にスクランブルを施すか否かが判定される（ステップS103）。

【0046】スクランブルを施す場合、CM付番組か否かが判定され（ステップS105）、CM付番組であれば、CM期間か否かが判定され（ステップS107）、CM期間であれば、広告情報源103からCMを選択し（ステップS109）、スクランブラ104においてスクランブルをOFFに設定し（ステップS111）、多重化装置105によりCMに鍵を多重化して（ステップS113）、セクタ106でCMを選択し、変調器109で変調してCMを出力する（ステップS115）。次いで、番組終了か否かを判定し（ステップS117）、終了してなければ、ステップS107に戻る。

【0047】ステップS105の判定において、CM付番組でなければ、従来と同様の課金管理処理が行われ（ステップS123）、管理装置107からの制御によりスクランブラ104においてスクランブルONが設定され（ステップS125）、番組が終了するまで（ステップS129）この番組を出力する（ステップS127）。

【0048】ステップS103の判定において、スクランブルを施さない番組であれば、スクランブラ104のスクランブルをOFFに設定して（ステップS131）、番組が終了するまで（ステップS135）この番組を出力する（ステップS133）。

【0049】次に、この第1の実施形態に対応した受信側の構成を図3に示す。図3において、受信端末装置201は、伝送路から入力される多数のチャンネルから所望のチャンネルを選択して選局復調する選局回路202と、選局回路202からの信号または外部入力信号を選択して出力する選択回路211と、CM期間の映像信号のブランキング期間に多重化された鍵及び制御コードを抽出する鍵抽出回路203と、この鍵及び制御コードを記憶するメモリ206と、この鍵を使用してスクランブルを解除するデスクランブラ204と、信号処理回路205と、コピーガード回路212と、リモコン受信機208と、端末制御回路207とを備えて構成されている。

【0050】また、これ以外に受信側には、TV受信機210と、リモコン送信機209とがある。ここでは受信端末装置201は例えばCATVのセットトップボックス、衛星放送の受信端末等のTV受信機210の外にある場合を示している。当然のことながらこれをTV受信機210に内蔵することも可能である。

【0051】次に、この受信端末装置201の動作を説明する。まず視聴者は見たい番組がある場合、リモコン送信機209を使用して視聴したいチャンネルを選択する。これをリモコン受信機208が受信すると端末制御回路207にこれを伝え、端末制御回路207は選局回路202を制御して指定されたチャンネルを選局し、選択回路203に出力する。この選局回路202にはチャンネルの選局と選局されたチャンネルの映像信号と音声信号を復調する回路が含まれている。選択回路211は外部入力との切替装置であり、VTR、DVD等の他の装置から入力する場合に切り替える。

【0052】選局回路202で選局されて復調された映像信号と音声信号は、抽出回路203を通してデスクランブラ204に入力される。抽出回路203は、映像信号のブランキング期間からデータを抽出し、図30に示すような同期コードを検出すると次に続く情報をメモリ206に書き込む動作を行う。

【0053】端末制御回路207はメモリに蓄えられた制御コードをもとに鍵が伝送されてきたことを検知し、CMが終了すると入手した鍵を使用してスクランブルがかけられた有料番組のデスクランブルが行えるようにデスクランブラ204の制御を行う。デスクランブラ204の出力は信号処理回路205で外部のTVに出力できるように信号処理され、さらにコピーガード回路212を介してTV受信機210に入り、画面上にデスクランブルされた番組が映し出される。

【0054】この場合の端末制御回路207の制御フローチャートを図17に示す。図17において、リモコン受信機208から端末制御回路207が選局要求を受けると、選局回路202に要求チャンネル選局の制御信号を送る(ステップS141)。次いで、この番組がスクランブルが施されているか否かを判定し(ステップS143)、スクランブルが施されていないければ、無料処理を行って(ステップS157)、終了する。

【0055】スクランブルが施されていれば、CM付番組か否かを判定し(ステップS145)、CM付でなければ、有料処理を行って(ステップS159)終了する。なお、有料処理の内容は従来技術と同様であるので省略する。

【0056】CM付番組であれば、CM期間か否かを判定し(ステップS147)、CM期間であれば、多重データを抽出し(ステップS149)、デスクランブラ204をデスクランブルOFFに設定し(ステップS151)、抽出された鍵および制御コードをメモリ206へ格納する(ステップS153)。次いで、番組が終了したか否かを判定し(ステップS155)、終了していないければ、ステップS147へ戻る。

【0057】ステップS147の判定において、CM期間でなければ、鍵がメモリ206に格納されているか否かを判定し(ステップS161)、鍵があればこれを用いてスクランブルの解除を行うべく、デスクランブラ204にデスクランブルONの制御信号を送り(ステップS163)、鍵がなければデスクランブラ204にデスクランブルOFFの制御信号を送り(ステップS165)、ともにステップS155へ移る。

【0058】こうして、CM期間中から有効な鍵を抽出すると、CM終了後デスクランブルされた有料番組が視聴可能になる。

【0059】このようなシステムにすることにより、CMを受信する必要性が生じ、CMによる広告効果があるため、このようなサービスの発展に寄与し、さらには料金の低下で視聴者にも還元されることになる。

【0060】さて、本発明では1つの有料番組に対してのCMの割合やCMの挿入頻度は任意に設定可能であり、番組の放映料、番組の視聴料金、視聴者の許容度に応じて設定する。

【0061】これは、図2の管理装置107からタイミング発生回路108の制御で設定でき、CMの放送時間については、例えば図4のグラフに示すようにCMの量を多くすればするほど料金を安くし、CMの量が少ない場合は料金を高くするというような形態が考えられる。

【0062】また、CMの挿入頻度については、図5に示すように大きく分けて2つ考えられる。1つは図5(a)の様に番組の直前にCMを挿入する方法であり、CMの時間は長い番組中にはCMが入らない構成であり、もう一つは図5(b)の様に1つの番組を適当な時

間単位に分割し、それらの間に短いCMを入れる構成である。これらは番組の内容等によって放送局側で使い分けられる。

【0063】さらに、このように1つの番組に対して何回かCMを挿入する場合、そのCMを単位に鍵を更新することにより秘匿性が向上するという効果もある。

【0064】以下、本発明の他の実施形態について説明する。上記の第1の実施形態ではCMが有料番組と同じ動画像を含むTV信号である場合の例を説明したが、次に、第2の実施形態としてCMをテキストなどのデータ量の少ない情報で伝送し、受信側でこれらの情報からCM画面を構成して表示する例について説明する。

【0065】第2の実施形態の放送局側の構成を図6に示す。第1の実施形態との相違は、広告情報源が映像・音声信号ではなく、テキスト形式であることと、番組とCMとのセレクタ106が無いことである。その他の第1の実施形態と同様の機能を持つものに関しては同じ符号を付与しており、機能的な説明は省略する。

【0066】広告情報源103として提供されるのは、テキストデータやそれに準じるデータであり、1つのCMを構成するデータ量は画像情報として供給された第1の実施形態に比べて非常に少ない。このデータはJAV A等のスクリプト言語で記述されたものでもよく、これらの言語を使用すれば端末側でスクリプトを解釈してアニメーション等の動画によるCMを表示することが可能になる。

【0067】第1の実施形態と同様に管理装置107の制御により映像番組とCMが選択され、映像番組の映像信号のブランキング期間に図26に示すように、制御コードの値によってCMか鍵かの区別がなされた形で多重化装置105によりCMと鍵が多重化され、変調器109を介して放送される。

【0068】この第2の実施形態の端末側の構成図を図7に示す。第1の実施形態との相違は、表示制御回路613及び混合回路614が付加されていることである。また図3と同じ機能を持つものには、同一の符号を付与しており、同様の機能を有するものとする。

【0069】視聴者のリクエストからチャンネルの選択までの制御は第1の実施形態と同様であり、抽出回路203で抽出されるデータにはCMデータまで含まれる点異なる。抽出回路203では映像信号からCMデータと鍵を抽出し、メモリ206に書き込む。

【0070】表示制御回路613は端末制御回路207の制御でメモリ206に蓄えられたCMデータを使用してCM画面を構築する。このCM画面はテキスト表示やスクリプト言語を解釈して構築した画面であり、表示制御回路613はこの構築した画面を混合回路614に出力し、適度な割合で受信した番組にCMを混合するように混合回路614を制御してCMを表示する。

【0071】デスクランブラ204は第1の実施形態と

同様に有効な鍵を入手する動作を開始し、混合回路 614 にデスクランブルした映像や音声信号を出力する。本実施形態における端末制御回路の制御フローチャートを図 24 に示す。

【0072】図 24 によれば、リモコン受信機 208 から端末制御回路 207 が選局要求を受けると、選局回路 202 に要求チャンネル選局の制御信号を送る（ステップ S341）。次いで、この番組がスクランブルが施されているか否かを判定し（ステップ S343）、スクランブルが施されていないければ、無料処理を行って（ステップ S345）、終了する。

【0073】スクランブルが施されていれば、CM 付番組か否かを判定し（ステップ S347）、CM 付でなければ、有料処理を行って（ステップ S349）終了する。なお、有料処理の内容は従来技術と同様であるので省略する。

【0074】CM 付番組であれば、多重データを抽出し（ステップ S351）、多重データの制御コードが CM を示すか否かを判定する（ステップ S353）。CM であれば CM 画面を構築し（ステップ S365）、CM 画面を表示し（ステップ S367）、次いで、番組終了か否かを判定し終了でなければステップ S351 へ戻る。

【0075】制御コードが CM でなければ、多重データが鍵か否かを判定し（ステップ S355）、鍵であれば鍵をメモリに保存し（ステップ S357）、次いで有効な鍵がメモリに有るか否かを判定し（ステップ S359）、鍵があればこれを用いてスクランブルの解除を行うべく、デスクランブラ 204 にデスクランブル ON の制御信号を送り（ステップ S361）、鍵がなければデスクランブラ 204 にデスクランブル OFF の制御信号を送り（ステップ S363）、ともにステップ S369 へ移る。

【0076】本実施形態では混合回路 614 の制御を制御することにより、CM を画面全体や画面の一部など表示位置や割合を任意に可変することができ、鍵が未入手でデスクランブルできないときは全画面に CM を表示し、次からは画面の一部に表示するなど様々な表示方法が考えられる。

【0077】図 8 は、本発明の第 3 の実施形態における放送局の構成を示す構成図である。第 1 の実施形態と異なる点は、有料番組が放送される第 1 のチャンネルとは異なる第 2 のチャンネルを設定し、このチャンネルで放送される CM に第 1 のチャンネルのデスクランブル鍵を多重化する点である。このため、第 1 のチャンネルに制御コードを多重化する多重化装置 711 と、第 2 のチャンネルのための変調器 710 とが付加されている。その他の図 2 と同様の機能を持つものには同一の符号を付与しており、それぞれの同様に機能を持つものとする。

【0078】本実施形態における多重化装置 711 では、図 27 に示すようなデータを有料番組の映像信号の

ブランキング期間に多重化して第 1 のチャンネルである CH1 で放送する。

【0079】このデータは、図 27 に示すように、同期コード、制御コード、CH-ID（チャンネル識別番号）、スクランブルフラグ、CM-CH 使用フラグ、CM-CH No.、およびパリティの各フィールドから構成されている。CH-ID は、番組が放送されるチャンネル自体の番号であり、スクランブルフラグはこの番組にスクランブルがかかっているかを示し、CM-CH 使用フラグは第 2 のチャンネルである CM チャンネルを使用するか否かを示すフラグであり、CM チャンネルの CM を使用する場合は CM-CH No. に使用するチャンネル番号を示す。

【0080】また、CM を放送するチャンネル（CHk とする）は第 1 の実施形態と同様に選択された CM に図 25 のようなデータを多重化し、変調器 710 を介して CHk の TV 信号として放送される。

【0081】図 18 は、第 3 実施形態の放送局の管理装置 107 の動作を説明するフローチャートであり、同図（a）は番組放送側の CH1 の制御系を示し、同図（b）は CM 放送側の CHk の制御系を示す。

【0082】まず、図 18（a）において、映像情報源 102 に対し番組選択を指示し、選択された番組の映像・音声信号が多重化装置 711 に与えられる（ステップ S171）。次いで、多重化装置 711 で補助データを多重化させ（ステップ S173）、この番組にスクランブルを施すか否かを判定する（ステップ S174）。次いで、スクランブルを施す場合には、スクランブラ 104 のスクランブルを ON に設定し（ステップ S175）、スクランブルを施さない場合には、スクランブラ 104 のスクランブルを OFF に設定する（ステップ S176）。次いで番組を CH1 で放送し（ステップ S177）、番組終了判定（ステップ S178）後、未了であれば、ステップ S177 へ戻る。

【0083】図 18（b）の広告放送チャンネルの制御は以下の通りである。まず、対応する番組にスクランブルが施されているか否かが判定され（ステップ S181）、スクランブルが施されていないければ、何もしないで終了する。スクランブルが施されていれば、CM 付番組か否かが判定され（ステップ S183）、CM 付番組でなければ、何もしないで終了する。CM 付番組であれば、広告情報源 103 から CM を選択し、その映像・音声信号が多重化装置 105 に与えられる（ステップ S185）。

【0084】次いで、多重化装置 105 により CM に鍵が多重化され（ステップ S187）、補助データが多重化され（ステップ S189）、変調器 109 により変調されて CHk で放送する（ステップ S191）。次いで、番組終了判定（ステップ S193）後、終了してなければ、ステップ S185 へ戻る。

【0085】この第3の実施形態に対応する受信側の構成自体は、第1の実施形態と同じであり、ここでは図3を使用して説明する。基本的に第1の実施形態と異なるのは端末制御回路207の制御アルゴリズムであり、ここを中心に説明する。

【0086】第1の実施形態と同様に、視聴者からリモコン送信機209を介してCH1を受信する要求が出されたとなると、端末制御回路207は選局回路202を制御してCH1を受信させ、抽出回路203にはCH1のTV信号が入力される。抽出回路203は、入力される映像信号のブランキング期間から図27に示した制御データを抽出し、メモリ206に格納する。

【0087】端末制御回路207は、メモリ206に格納された制御データ中のスクランブルフラグ、CM-CH使用フラグを参照し、両フラグが共にセットされているとCM付で料金を安くする本発明の有料番組であると判断し、選局回路202を制御してCHkを選局し、このチャンネルで放送中のCMをTV受信機210で映し出す制御を行う。

【0088】すると今度は抽出回路203でCM中に多重化されているデータが抽出され、メモリ206に格納される。CMには図25に示すようなデータが多重化されているので、メモリ206に格納されるデータは、CH関連情報に対応するチャンネル番号にCH1の番号があるときの鍵データである。

【0089】この鍵を入手すると、再度選局回路202を制御してCH1を受信し、入手した鍵を使用してデスクランブラ204を動作させ、TV受信機210にはデスクランブルされたCH1の有料番組が映し出される。この制御フローチャートを図19に示す。点線内がCM付の番組を受信した時の処理になる。

【0090】図19によれば、リモコン受信機208から端末制御回路207が選局要求（これをCH1とする）を受けると、選局回路202にCH1選局の制御信号を送りCH1を選局させる（ステップS201）。CH1が選局されると、CH1の復調信号が選択回路211を介して抽出回路203に与えられる。次いで、CH1に多重化されたデータを抽出回路203により抽出し、CH-ID、スクランブルフラグ、CM-CH使用フラグ、およびCM-CH No. をメモリ206に格納する（ステップS203）。

【0091】次いで、スクランブルフラグによりこの番組にスクランブルが施されているか否かを判定し（ステップS205）、スクランブルが施されていないければ、無料処理を行って（ステップS221）、終了する。

【0092】スクランブルが施されていれば、CM-CH使用フラグによりCM付番組か否かを判定し（ステップS207）、CM付でなければ、有料処理を行って（ステップS223）終了する。なお、有料処理の内容は従来技術と同様であるので省略する。

【0093】CM付番組であれば、既に鍵がメモリ206に格納されているか否かを判定し（ステップS209）、鍵があれば、CH1に選局を戻し（ステップS225）、スクランブルを解除するためにデスクランブラ204をデスクランブルONに設定し（ステップS227）、番組が終了したか否かを判定し（ステップS219）、終了していなければ、ステップS209へ戻る。

【0094】ステップS209の判定において、鍵がなければ、CM-CH No. によりCMのチャンネル番号CHkを入手して、選局回路202にCHk選局の制御信号を送りCHkを選局させる（ステップS211）。CHkが選局されると、CHkの復調信号が選択回路211を介して抽出回路203に与えられる。次いで、CHkに多重化されたデータを抽出回路203により抽出し（ステップS213）、デスクランブルをOFFに設定し（ステップS215）、鍵をメモリ206に保存し、番組が終了したか否かを判定し（ステップS219）、終了していなければ、ステップS209へ戻る。

【0095】次に、この第3の実施形態の変形例として、CM付で料金を安くするチャンネルが複数存在する場合の放送局の構成を図9に示す。図8に対して図9の変形例では、映像情報源102、多重化装置711、スクランブラ104、及び変調器109が複数組設けられ、これらの符号にはそれぞれの組を示すaからnの添え字が付加されている。なお、図8と同じ符号を付してある構成要素には同じ機能を果たすものとする。

【0096】CH1からCHkの各チャンネルで放送される番組には、多重化装置711で前述の図26のフォーマットで補助データが多重され、CMチャンネル（CHk）は図27に示すデータが多重され、図28に示すようにCH1からCHnに対応したCM1からCMnが繰り返し順次放送される。

【0097】受信側の処理は上述の処理と全く同じであり、CH1からnまでのいずれかのチャンネルを選局し、選局したチャンネルの映像信号から抽出したデータに従って、CMチャンネルの選局、データの抽出が行われ、抽出した鍵を使用してデスクランブラ204が動作し、デスクランブルされた番組がTV受信機210に映し出される。

【0098】さて、このようなシステムにおける端末制御回路207の制御についてさらに説明を加える。CMのチャンネルを受信して入手した鍵は、たとえば図29のようにメモリ内に各チャンネルとそれぞれに対応した鍵、更新日時等が記録されており、新しく有効な鍵かが受信されるまで保持される。

【0099】つまり、初期状態からCH1を受信している状態で、途中でCH2に切り換えたとなると、CH2がCH1と同様にCMの視聴を必要とする場合は上記の例の手順で鍵を入手し、メモリに記録し、CH2をデス

クランブルするが、その後CH1に戻った場合を考える。このときメモリ内に記録されている鍵の更新日時と有料番組内に多重されている鍵の使用期限を比較して、使用期限を過ぎていなければメモリ内に記録されている鍵を使用し、期限を過ぎている場合は再度鍵の入手手順から動作を行うように制御される。

【0100】また、第3の実施形態のような手順で動作する受信端末装置は、図7に示すように表示制御回路613、混合回路614を加えることにより、上記制御によりチャンネルを切り換えてCMを表示する場合には、これを視聴者に表示するような変形も実現可能になる。この変形例のCM付番組処理部分のフローチャートを図20に示す。基本的な流れは図19と同じなので、CM付番組処理の部分（図19のステップ209以下の部分に相当）だけを示している。

【0101】図20によれば、CM付番組の場合、有効な鍵がメモリ206に格納されているか否かが判定され（ステップS231）、鍵がなければ選局回路202にCM放送チャンネルであるCHkを選局させる（ステップS233）。そして、抽出回路203に多重データを抽出させ（ステップS235）、抽出されたデータに基づいて表示制御回路613により構築されたCM画面を混合回路614により映像信号に混合して画面表示させる（ステップS235）。

【0102】次いで、デスクランブラ204をデスクランブルOFFに設定し（ステップS239）、多重データに鍵があればメモリ206に格納し（ステップS241）、番組終了か否かを判定し（ステップS243）、終了でなければステップS231へ戻る。

【0103】ステップS231の判定において鍵があれば、選局回路202にCH1を選局させ（ステップS245）、デスクランブラ204をデスクランブルONに設定し（ステップS247）、番組終了か否かを判定し（ステップS243）、終了でなければステップ231へ戻る。

【0104】さらに上述の様に番組の途中でチャンネルを切り換えて、今までに受信した鍵が無効になったときに、再度CMを受信するか、料金を支払って視聴するかを選択をTV画面に表示し、リモコンを介して受信した視聴者の選択結果をもとに制御を行うことも可能になる。この制御フローチャートを図21に示す。基本的な流れは図19と同じなので、CM付番組処理の部分（図19のステップ209以下の部分に相当）だけを示している。

【0105】図21において、CM付番組の場合、有効な鍵がメモリ206に格納されているか否かが判定され（ステップS251）、鍵がなければ、再度CMを受信するか、料金を支払って視聴するかを選択をTV画面に表示する（ステップS253）。視聴者はこの画面を見て、CM受信するか有料視聴するかを選択を行い、リモ

コンを介して応答する。

【0106】次いで、端末制御回路207は、この応答がCM受信か否かを判定し（ステップS255）、CM受信であれば、選局回路202にCHkを選局させ（ステップS257）、抽出回路203に多重データを抽出させ（ステップS259）、デスクランブラ204をデスクランブルOFFに設定し（ステップS261）、多重データに鍵があればメモリ206に格納し（ステップS263）、番組終了か否かを判定し（ステップS265）、終了でなければステップ251へ戻る。

【0107】ステップS251の判定において鍵があれば、選局回路202にCH1を選局させ（ステップS269）、デスクランブラ204をデスクランブルONに設定し（ステップS271）、番組終了か否かを判定し（ステップS265）、終了でなければステップ251へ戻る。

【0108】ステップS255の判定において、CM受信でなければ、課金処理を行って（ステップS267）ステップS269へ移る。

【0109】また、第1の実施形態においても図10に示すように多重化装置711で図26に示すようなデータを挿入する構成にすることにより、端末側で通常の有料放送かCM付の有料放送かを検知することができるようになり、有料／無料など様々な番組が放送できるようになる。

【0110】次に、第1の実施形態と第3の実施形態をあわせた第4の実施形態について説明する。これは鍵を多重化したCMを有料番組中に挿入すること基本にして、予備としてCMを放送するチャンネルにも同じデータを多重化するものである。

【0111】この第4の実施形態における放送局側の構成例を図11に示す。図2、図8、図10の各図の構成品と同じ機能をもつ構成品には同一の符号を付しており、重複する説明を省略する。第1の実施形態と同様に、CH1では任意のタイミングで鍵を多重化したCMが挿入された番組が放送され、この鍵を多重化したCMは第3の実施形態と同様にCHkでも放送される。

【0112】受信端末側の構成は図3と同じであり、端末制御回路207の制御方法が異なり、この制御フローチャートを図22に示す。

【0113】ここでCH1とCHkは、図30に示す様な配列によりCMや番組が放送されているとする。そして、もし視聴者が図中の時刻AのようなCM期間中ではない番組期間中にCH1を選択したとすると、このCH1では時刻Bになるまで鍵が伝送されないため、CH1を受信したTV信号のスクランブルは時刻Bまで解除できないことになる。

【0114】そこで時刻AでCH1を選局した場合は、一時的に受信チャンネルをCHkに切り換えて、CHkで放送されるCM-1を表示させるとともに有効な鍵を

10

20

30

40

50

入手し、CM-1が終了するとともにCH1に復帰するように制御することにより、番組が途中の場合でもスムーズに番組を受信することができる。

【0115】さて、現在では地上波や衛星の放送局と各視聴者の間には電話を使って双方向通信路を確保し、CATVにおいては電話に加えて、自身のケーブルを使って双方向の通信路を確保し、インタラクティブな放送を行う事業者も増えてきた。これらの放送の例として視聴者参加のクイズ番組やビデオオンデマンド等のオンデマンドサービスがあげられる。

【0116】次に、このビデオオンデマンド等のオンデマンドサービスを行う場合を第5の実施形態として説明する。図12は第5の実施形態の放送局側の装置構成を示す図であり、第1の実施形態の変形例を示す図10との相違は、新たに通信制御装置1101が付加された構成になっており、その他の構成は図10と同様であり、同様の機能を持つ構成要素には同じ符号を付与して説明を省略する。

【0117】この通信制御装置1101は例えば電話機能を備えたものであり、放送チャンネルとは独立した伝送路を用いて、各視聴者との通信および通信制御を行う。なお、伝送路がCATVの場合には、電話のために公衆回線を利用することなく、CATVと同一ケーブルの通信路を使用することが望ましい。

【0118】また、図13はこの第5の実施形態の受信端末装置の構成を示しており、図3に対して通信制御回路1201が付加された構成になっており、その他の構成は図2と同様である。この通信制御回路1201は例えば電話機能を備えたものであり、放送局との通信を行って、オンデマンド番組のリクエストやインタラクティブな番組対するリアクションとして使用される。

【0119】ここで、視聴者がオンデマンドで映画等の番組をリクエストして視聴する場合を例として、本実施形態の動作を説明する。視聴者はオンデマンドの番組リクエストをリモコン送信機209を介して受信端末装置201に伝える。リクエストを受けた端末制御回路207は、指定されたチャンネルを選局するように選局回路202を制御し、選局されたチャンネルでは、まず図33に示すようなメニュー画面が放送される。これは番組の選択と視聴方法を決定するためのものであり、視聴者はリモコン送信機209を使って見たい番組と視聴方法を決定する。

【0120】ここで番組101をCM付の放送で視聴することを選択した場合、この視聴条件を示すデータが通信制御回路1201によって放送局に送信される。放送局側の通信制御装置1101でこのデータを受信すると、映像情報源102から指定された番組を選択して第1の実施形態と同様に番組中に鍵を多重したCMを挿入しながら放送を行い、受信側では番組の放送が始まると第1の実施形態に示した処理を行い、リクエストした番組

組を視聴する。本実施形態の端末側の制御フローチャートを図23に示す。

【0121】また、本実施形態においてもCMを視聴しない限り、スクランブルを解くことができないため、途中でチャンネルを切り換えるとスクランブルが解けなくなる。そこでこのような状態になったときは通信制御回路1201を介して端末側から放送局側に伝えたと番組が一時停止し、図34に示すようなメニュー画面が表示される。ここで再度CMを視聴することを選択すればCMから再送され、CMなしを選択すると番組は通常の有料番組として取り扱われる。

【0122】この場合と最初のメニューでCMなしを選んだ場合は受信端末装置と放送局の通信により、放送局の管理装置107で課金管理が行われるとともに鍵をこの通信路を使って端末側に送信し、端末側ではこの鍵を使ってデスクランブルした映像と音声の表示を行うことになる。

【0123】また、番組内容によっては、視聴者側からの要求として番組の途中はCMを入れてほしくないという場合がある。この場合番組の最初にCMを放送してしまうことが考えられるが、この場合CMの時間が長くなり本発明によって他のチャンネルに切り換えるということとはできないが、TVの前から離れてしまう可能性が残る。

【0124】これに対して図31の様にCMの期間の任意の時点で視聴者からのデータ入力を要求し、双方向通信路を介して放送局側でデータ入力を確認されると鍵を多重したCMを放送するようにすることで、ある程度CMを視聴者に視聴させることができる。

【0125】さて、ここまでは放送系について説明してきたが本発明はVTRやDVDなどの記録メディアを使用したパッケージソフトに対しても有効であり、その1つの例を第6の実施形態として説明する。

【0126】図14にはこのようなメディアに番組を記録する製作会社の装置構成を示しており、図10に示す放送局の装置構成図と同じ機能を持つものには同一符号を付してあり説明は省略する。製作会社1301では第1の実施形態における制御と同様に管理装置107の制御で映像情報源102から適切な番組を選択し、スクランブラ104で映像や音声にスクランブルを施す。また、広告情報源103から適切なCMを選択してスクランブルを施した映像や音声をデスクランブルする鍵を多重化し、セクタ106で任意のタイミングや頻度で番組にCMを挿入して記録装置1201に出力する。

【0127】この記録装置1201はセクタ106からの信号をビデオカセットやDVDなどの記録メディアに直接記録したり、マスターテープに記録する。マスターテープを作成した場合には、このマスターテープから更に市販用のビデオカセットにコピーしたり、DVDのプレス原盤を作成する。

【0128】このようにして製作されたビデオカセットやDVDなどの記録メディアは流通経路を通して、視聴者の手に届くことになる。

【0129】これらのメディアを入手した視聴者はそれぞれのメディアに対応した再生装置の出力を図3示す外部入力に接続し、再生を行う。受信端末装置201における処理は選択回路が外部入力の信号を選択する以外は第1の実施形態と同じであり、CMを視聴することにより記録された番組を正常に視聴することが可能になる。

【0130】特に、記録メディアは再生が視聴者にゆだねられるため、本実施形態の様な処理をしないでCMを挿入しても早送り等で視聴されない可能性があり、広告効果は低くなる。しかし、本発明によるとCMは必ず視聴されるため広告効果が上がり、これによりスポンサーもこのサービスに出費するようになり、このような記録メディアを安く視聴者に提供することができるようになる。

【0131】ここまで鍵の多重を映像信号のブランキング期間に多重する例を示してきたが、BS放送では音声信号中のデータパケットに多重され、デジタル放送においてはストリームのデータパケットの領域に多重されて伝送される。このようにメディアによって多重する領域は異なるが、以上説明した本発明はいずれのメディアでも実施可能である。

【0132】ここでスクランブルシステムについて少し説明を加える。図15にBS放送で使用されている鍵システムを示す。

【0133】放送局1401では映像信号と音声信号をそれぞれ映像スクランブラ1403、音声スクランブラ1404で擬似乱数（以下、擬似乱数をPNと省略する）発生器1405で発生するPNに従ってスクランブルが施される。このPN発生器1405に設定される初期値がスクランブル鍵Ksとして使用される。このスクランブル鍵Ksは1から数秒程度で更新し、これを更新周期の長いワーク鍵Kwで暗号化して多重化装置1407で多重する。さらにワーク鍵は端末毎に固有な鍵マスタ鍵Kmで暗号化して同じく多重化装置1407で多重されて伝送される。

【0134】端末装置1402ではマスタ鍵Kmを使用して復号器1418でワーク鍵Kwを復号し、ワーク鍵Kwを使用してスクランブル鍵Ksを復号し、このスクランブル鍵Ksを使用してPN発生器1415を動作させて、デスクランブラ1413、1414からはデスクランブルされた映像信号と音声信号が出力される。

【0135】契約条件比較回路1417ではマスタ鍵Kmで復号した契約内容とワーク鍵Kwで復号した番組の識別に基づいて受信可能か否かのチェックを行う。

【0136】本発明もこのような3層構造を持った鍵システムに適用可能であり、ここまで説明したCM期間に多重する鍵はワーク鍵Kwに相当する鍵とすることがで

き、ある程度更新周期の長い鍵であることが望ましい。

【0137】このように日本のBS放送では映像信号はラインローテーション、音声信号にはPN加算方式のスクランブルであるが、本発明ではいずれのスクランブル方式にも対応可能であり、CATV等で伝統的に行われているシンク圧縮方式等のアナログスクランブル方式、デジタル放送で行われているDESやマルチ2などのブロック暗号方式などスクランブル方式によらず適用される。

【0138】たとえば映像、音声情報源102、103がデジタルデータであり、スクランブラ104をブロック暗号方式（マルチ2）にすることによりCSデジタル放送システムにも適用可能になる。

【0139】

【発明の効果】以上説明したように請求項1に記載の本発明によれば、放送または記憶媒体を介して提供される映像ソフトウェアのスクランブル解除のための鍵をCM期間に多重化することにより、CMを視聴しないかぎり映像ソフトウェアのスクランブルが解けないため、CM付有料メディアにおけるCM視聴を保証することができ、映像ソフトウェアにCMを挿入して安く提供するサービスに参加するスポンサーが増え、最終的には料金引き下げが可能となるという効果がある。

【0140】また、請求項2ないし請求項5に記載の本発明によれば、テレビジョン番組にスクランブルを施すとともに、このスクランブルを解除する鍵をテレビジョン番組中に挿入されるCMに多重化することにより、鍵を入手するためにはCM視聴が必須となり、CM視聴率を高めてスポンサーの参加を促進するという効果がある。

【0141】また、請求項6ないし請求項10に記載の本発明によれば、有料番組を視聴するために第1のチャンネルを選択したときに番組の途中でCM期間でない場合に、番組中に挿入された次のCM期間を待つことなく、第2のチャンネルで放送されているCMを直ちに視聴して鍵を入手し、第1のチャンネルに復帰してスクランブルを解除することができるので、視聴者を待たせることがなくなるという効果がある。

【0142】また、請求項11に記載の本発明によれば、有料番組の規定料金か、CMを視聴して規定料金より低価格を選ぶかの選択を視聴者に提供することができるという効果を奏する。

【0143】また、請求項12ないし請求項14に記載の本発明によれば、CM期間中でなくても、番組放送チャンネルに多重化されたCMを構成するためのデータからCM画面を構成して表示するとともに、同様に多重化された鍵を入手することができるので、他チャンネルを使用することなく、また視聴者を待たせることなく、CM表示と鍵の入手ができるという効果を奏する。

【0144】また、請求項15に記載の本発明によれ

ば、オンデマンド方式のテレビジョン番組において、CMなしの規定料金か、CM付で無料かの選択を視聴者に提供することができるという効果がある。

【0145】また、請求項16に記載の本発明によれば、従来のBS放送で使用されているデスクランブル鍵の伝送方式を本発明のデスクランブル鍵の伝送に用いることができるという効果がある。

【図面の簡単な説明】

【図1】本発明に係るスクランブル方式の原理を説明する原理説明図である。

【図2】第1の実施形態の放送局側の構成を示す装置構成図である。

【図3】第1の実施形態の受信側の構成を示す装置構成図である。

【図4】CM量と料金設定との関係の例を示すグラフである。

【図5】1つの番組に対するCMの入れ方の例を示す図であり、(a)番組前にCMをまとめて入れる例、(b)番組前および番組中に分散してCMを入れる例である。

【図6】第2の実施形態の放送局側の構成を示す装置構成図である。

【図7】第2の実施形態の受信側の構成を示す装置構成図である。

【図8】第3の実施形態の放送局側の構成を示す装置構成図である。

【図9】第3の実施形態の放送局側の構成を示す装置構成図である。

【図10】第1の実施形態の変形例の放送局側の構成を示す装置構成図である。

【図11】第4の実施形態の放送局側の構成を示す装置構成図である。

【図12】第5の実施形態の放送局側の構成を示す装置構成図である。

【図13】第5の実施形態の受信側の構成を示す装置構成図である。

【図14】第6の実施形態である記憶媒体に本発明を適用した例を説明する装置構成図である。

【図15】有料放送の鍵システムを説明するシステム構成図である。

【図16】第1の実施形態の放送局側の動作を説明する制御フローチャートである。

【図17】第1の実施形態の受信側の動作を説明する制

御フローチャートである。

【図18】第3の実施形態の放送局側の動作を説明する制御フローチャートである。

【図19】第3の実施形態の受信側の動作を説明する制御フローチャート(その1)である。

【図20】第3の実施形態の受信側の動作を説明する制御フローチャート(その2)である。

【図21】第3の実施形態の受信側の動作を説明する制御フローチャート(その3)である。

10 【図22】第4の実施形態の受信側の動作を説明する制御フローチャートである。

【図23】第5の実施形態の受信側の動作を説明する制御フローチャートである。

【図24】第2の実施形態の受信側の動作を説明する制御フローチャートである。

【図25】多重データの例を示す図である。

【図26】多重データの例を示す図である。

【図27】多重データの例を示す図である。

20 【図28】CMを放送するチャンネルの放送順序の例を示す図である。

【図29】受信端末のメモリに蓄えられるデータの例を示す図である。

【図30】第4の実施形態におけるデータの多重例を示す図である。

【図31】第4の実施形態におけるデータの多重例を示す図である。

【図32】多重化データの各制御コード毎の制御の内容を示す表である。

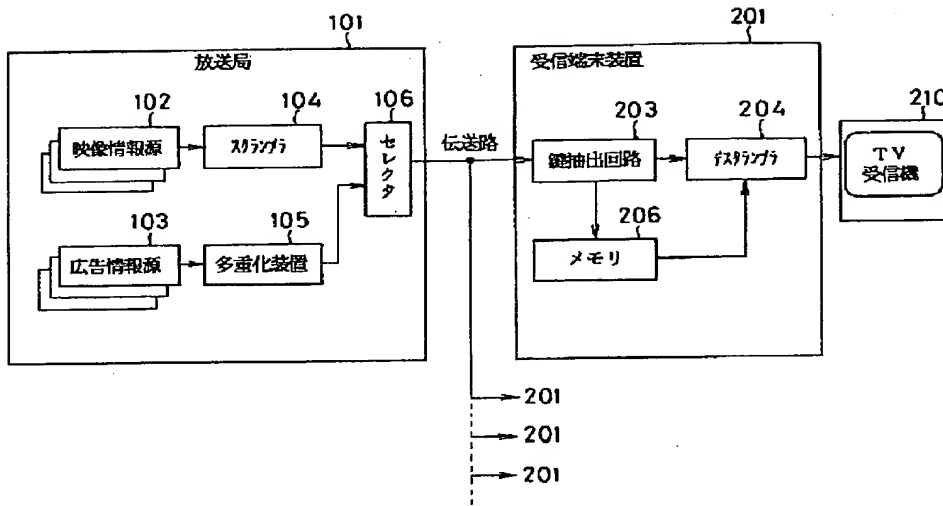
30 【図33】第5の実施形態で表示される画面の例を示す図である。

【図34】第5の実施形態で表示される画面の例を示す図である。

【符号の説明】

101…放送局、102…映像情報源、103…広告情報源、104…スクランブラ、105…多重化装置、106…セクタ、107…管理装置、108…タイミング発生器、109…変調器、201…受信端末装置、202…選局回路、203…鍵抽出回路、204…デスクランブラ、205…信号処理回路、206…メモリ、207…端末制御回路、208…リモコン受信機、209…リモコン送信機、210…TV受信機、211…選択回路、212…コピーガード回路。

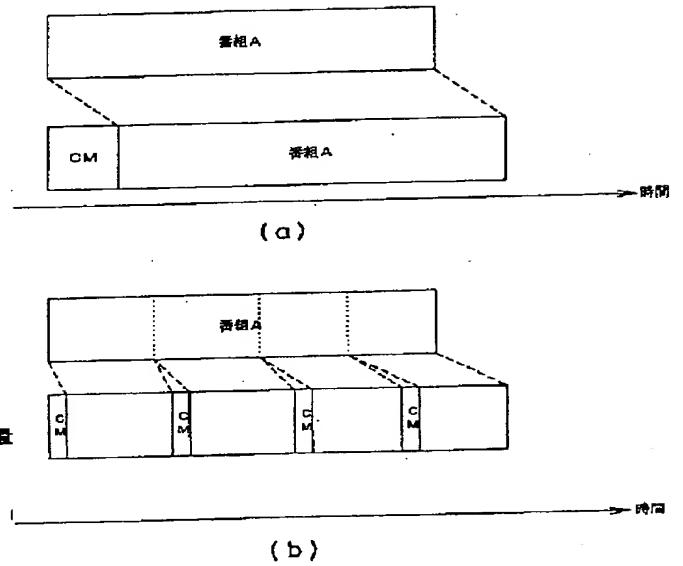
【図 1】



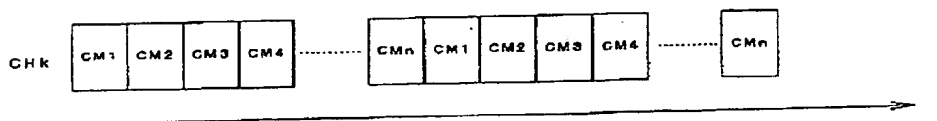
【図 4】



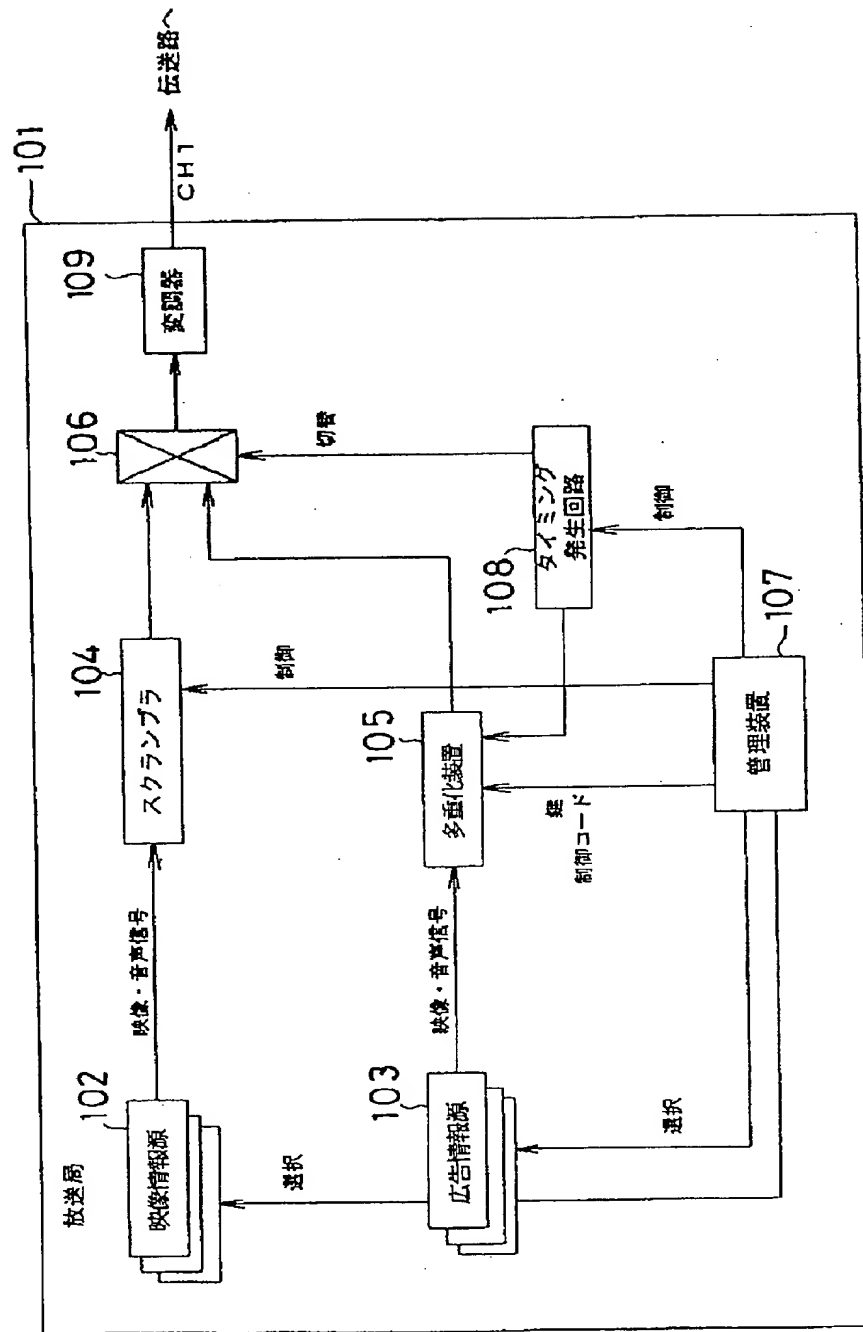
【図 5】



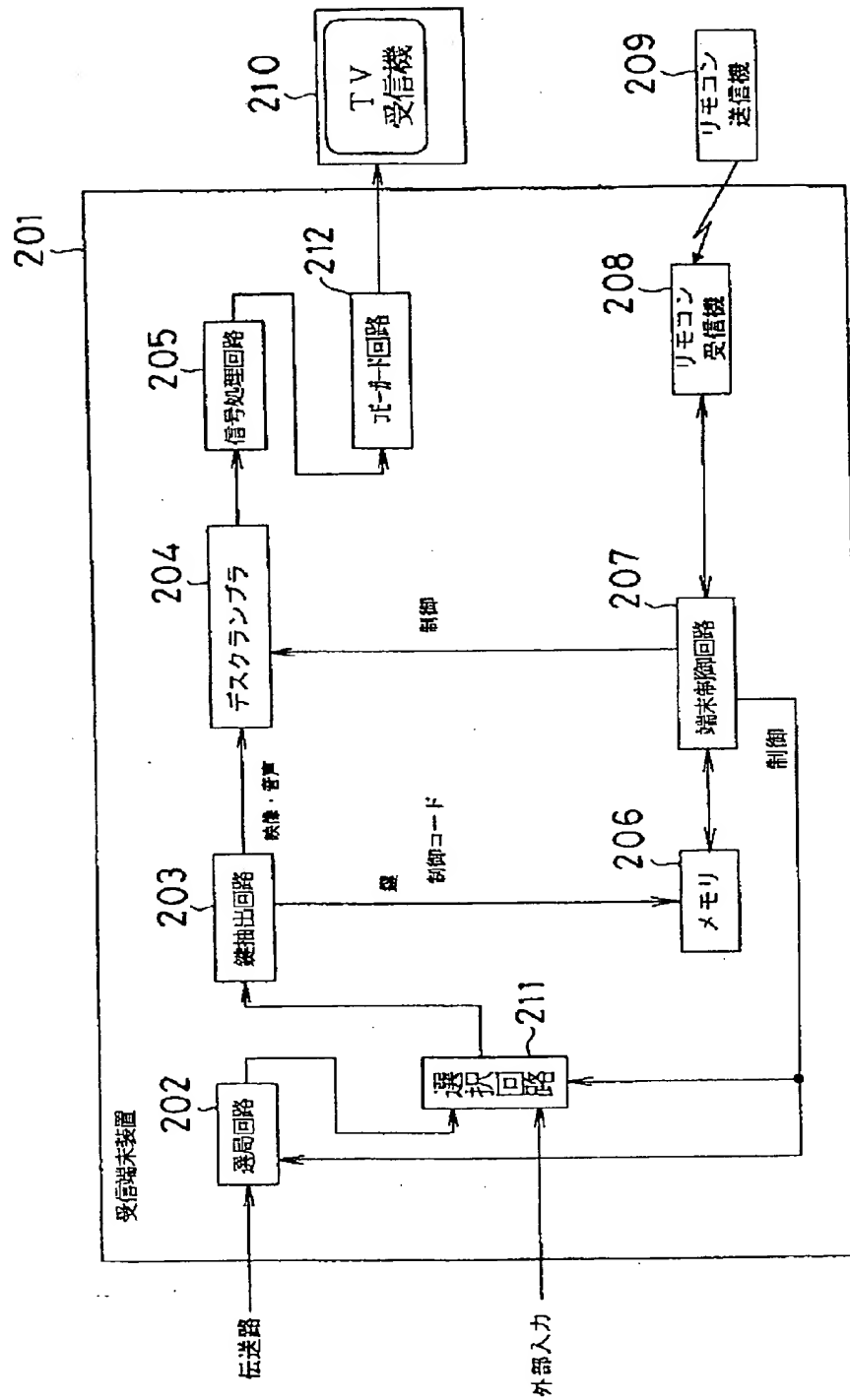
【図 28】



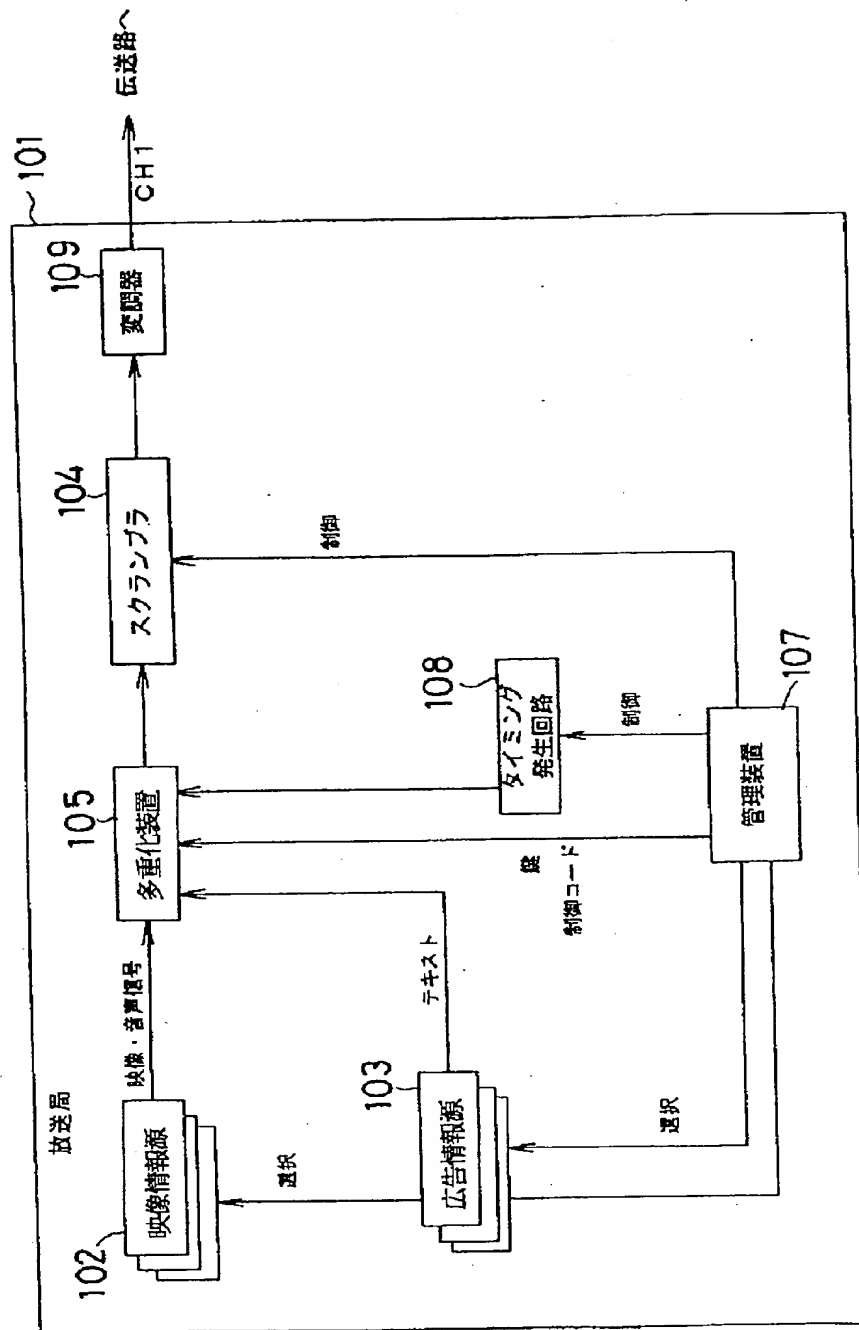
【図 2】



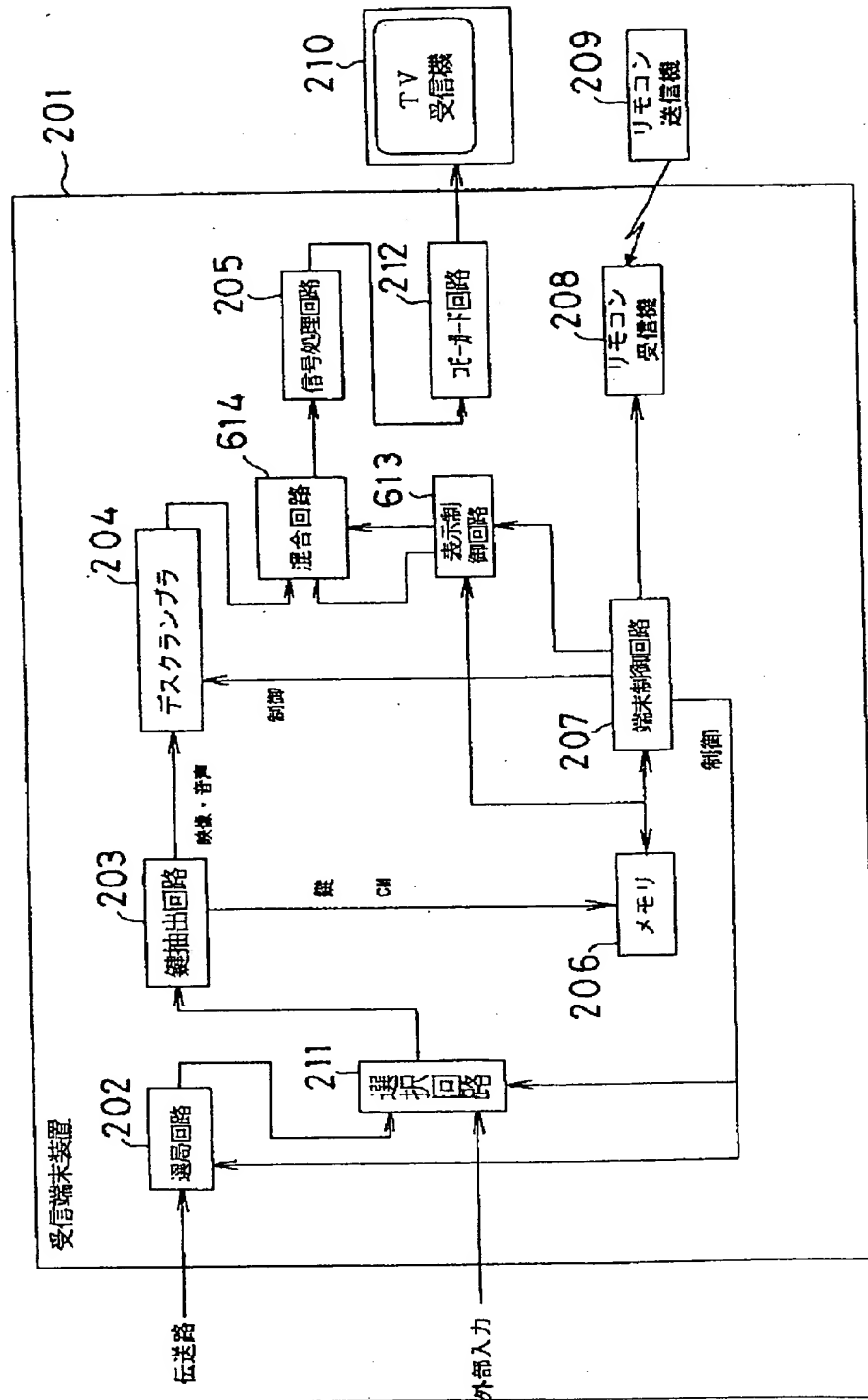
【 図 3 】



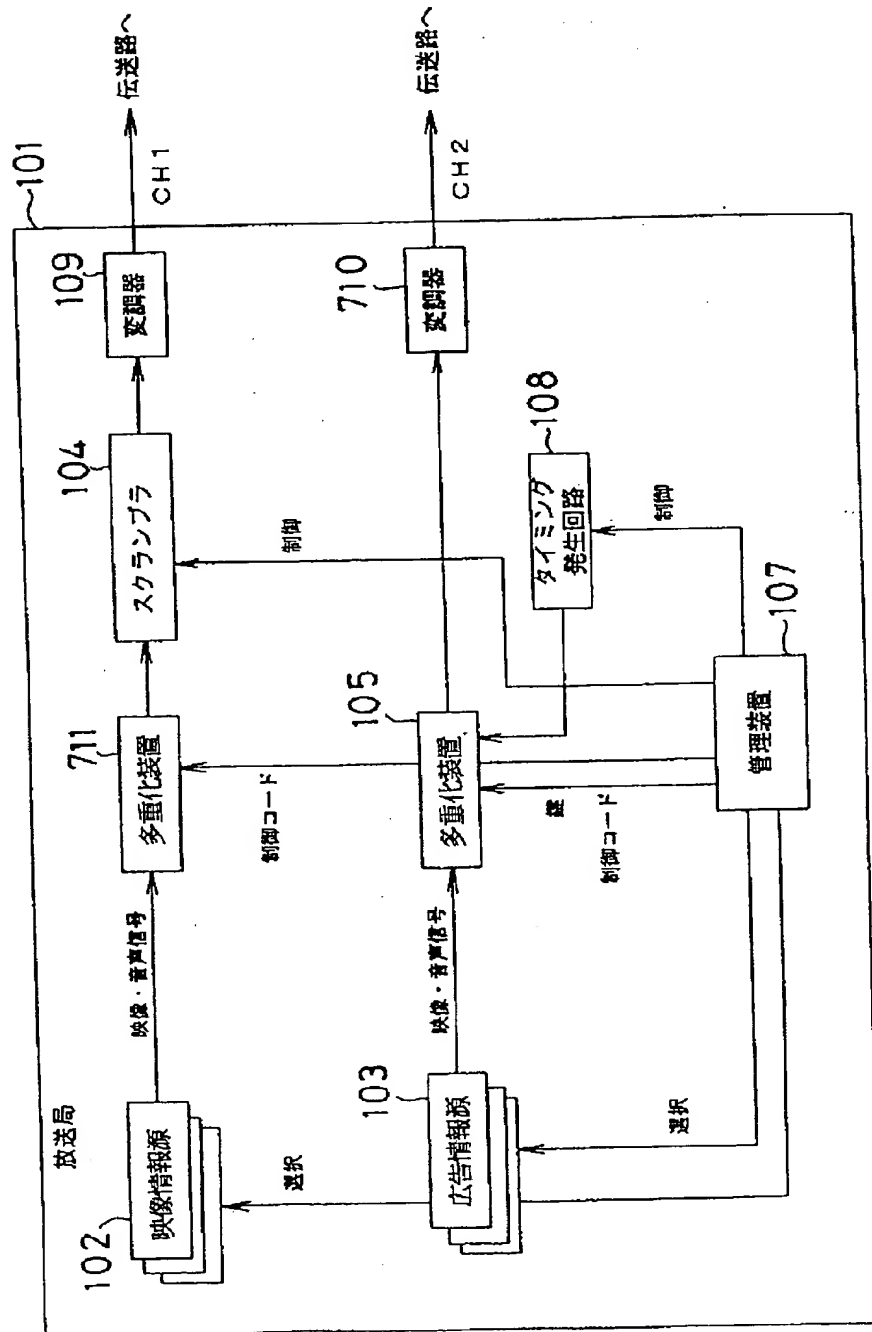
【図 6】



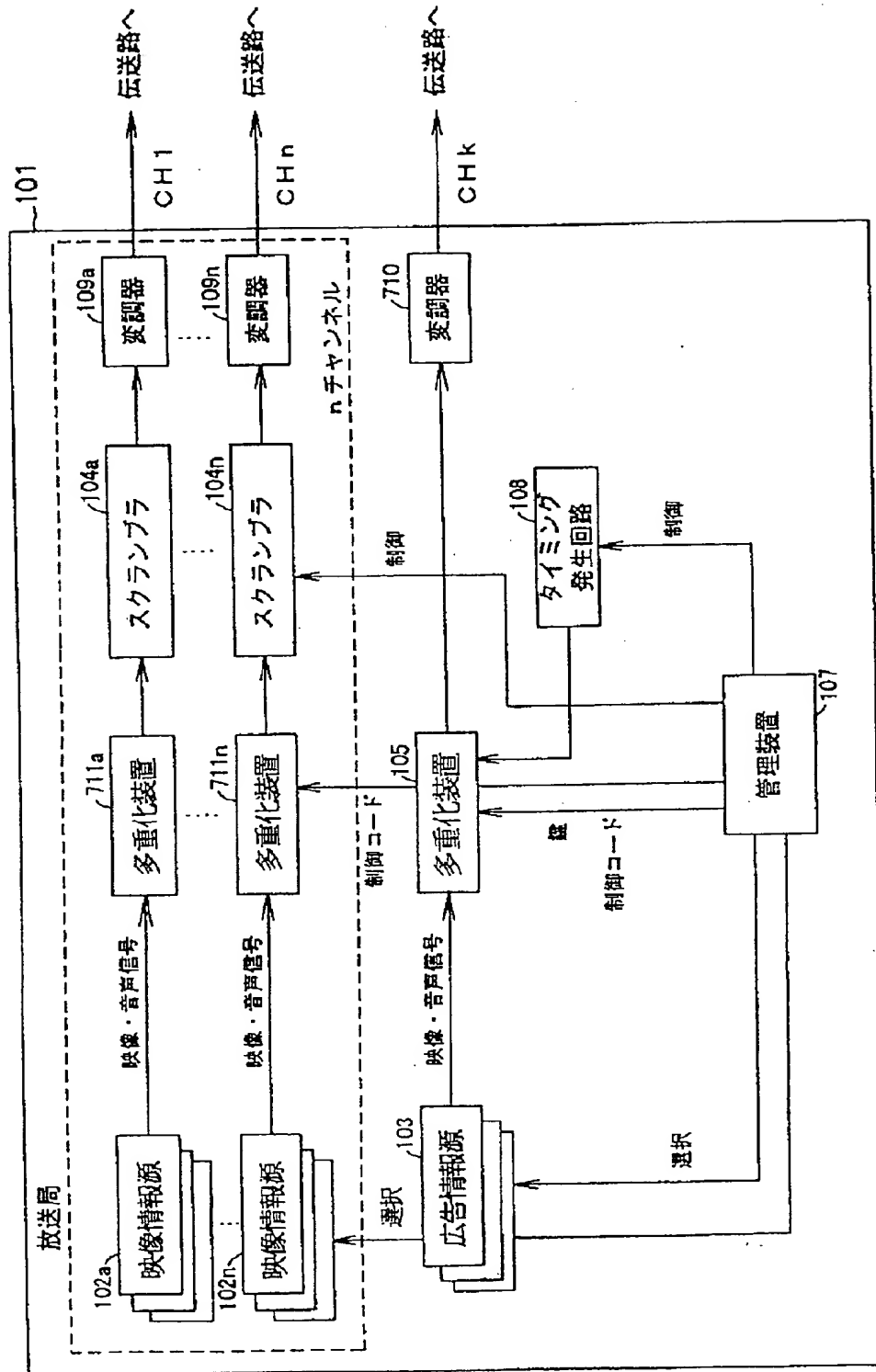
【 図 7 】



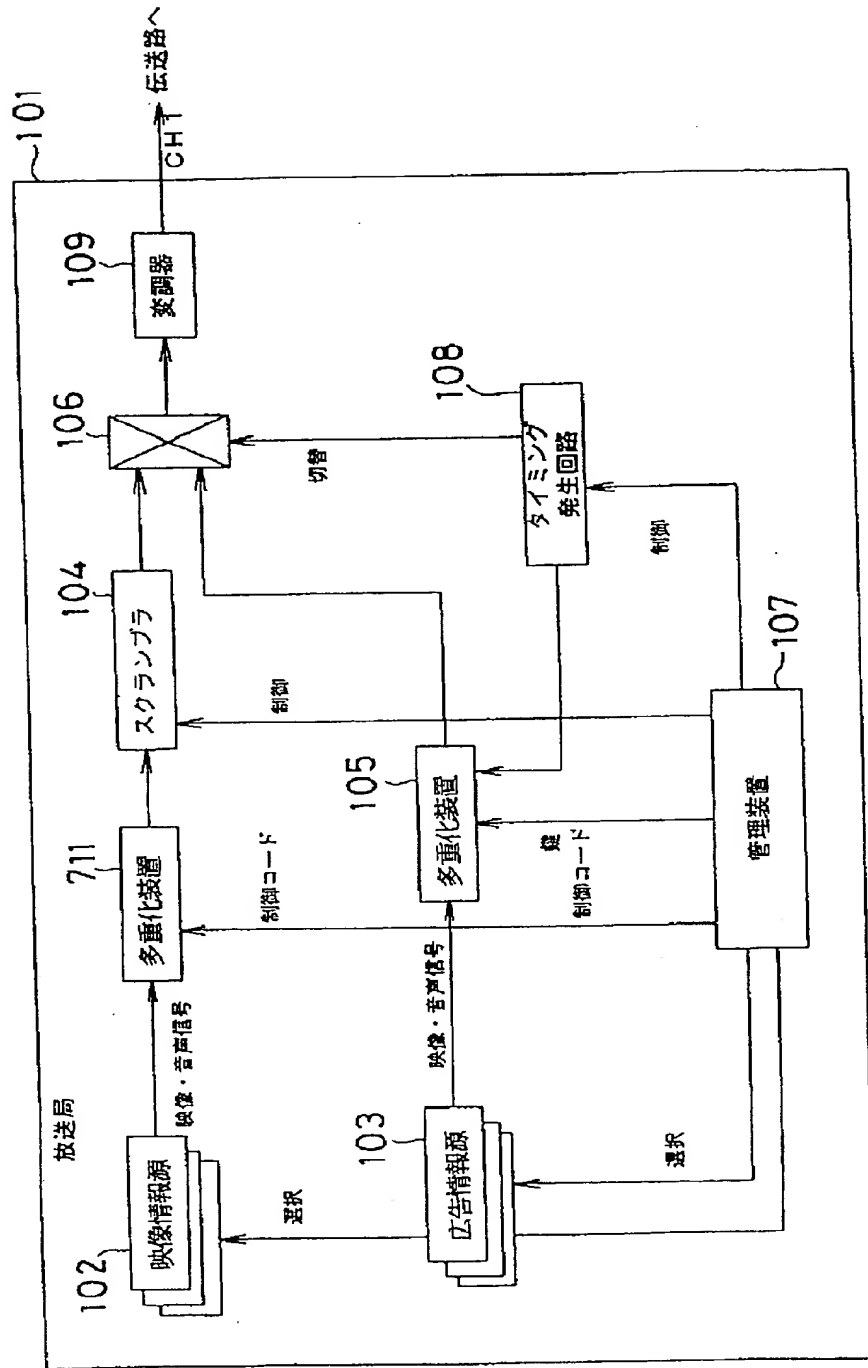
【図 8】



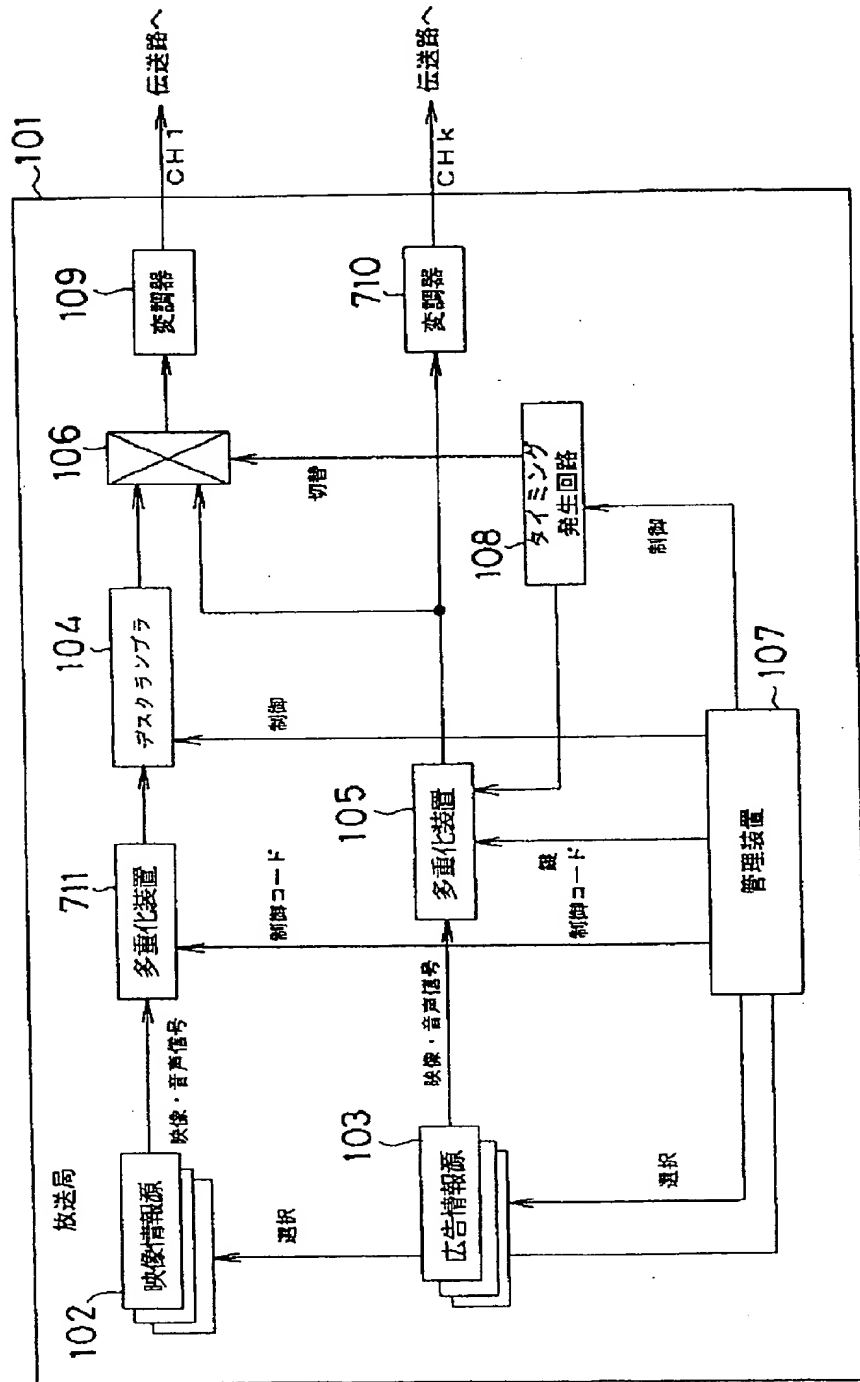
【図 9】



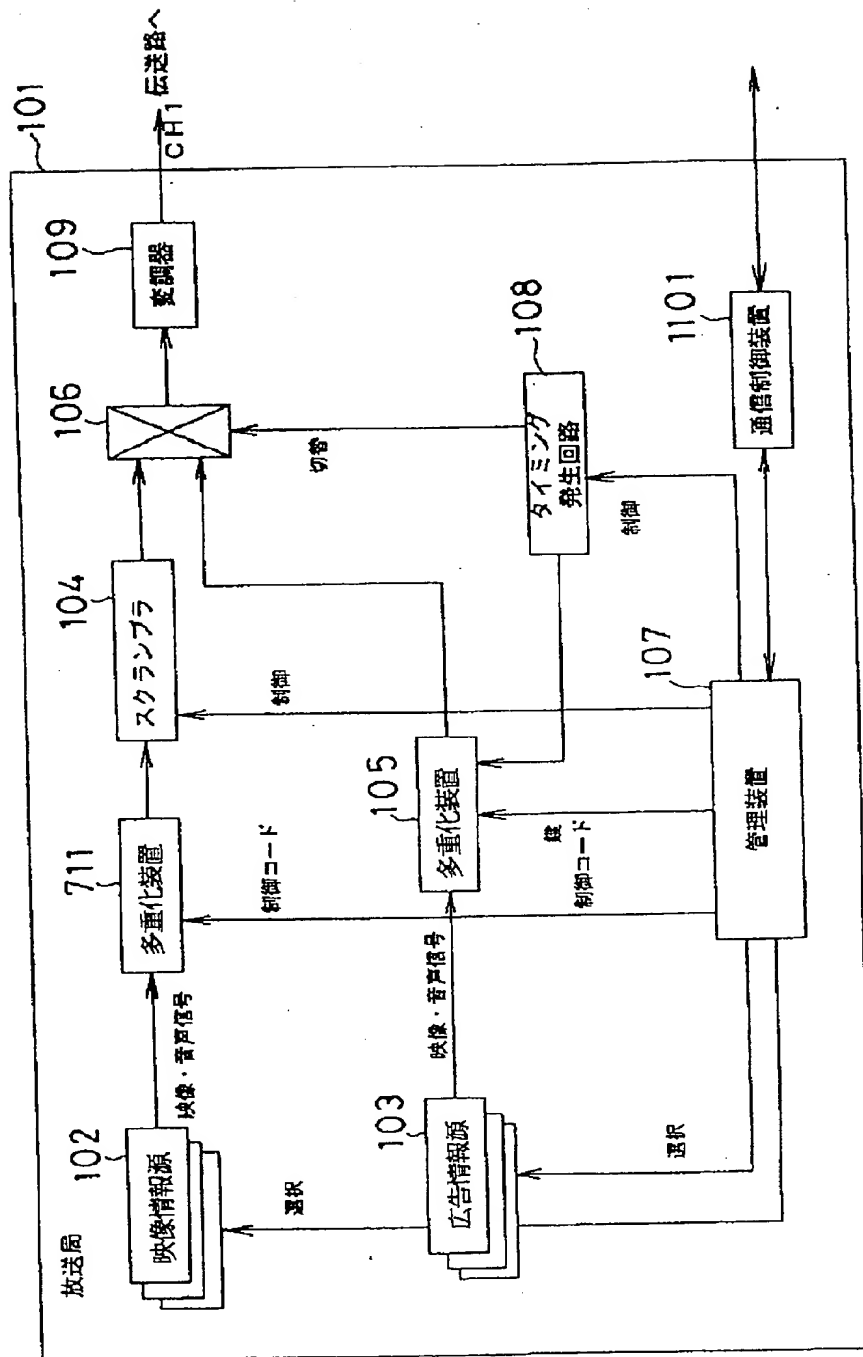
【図 10】



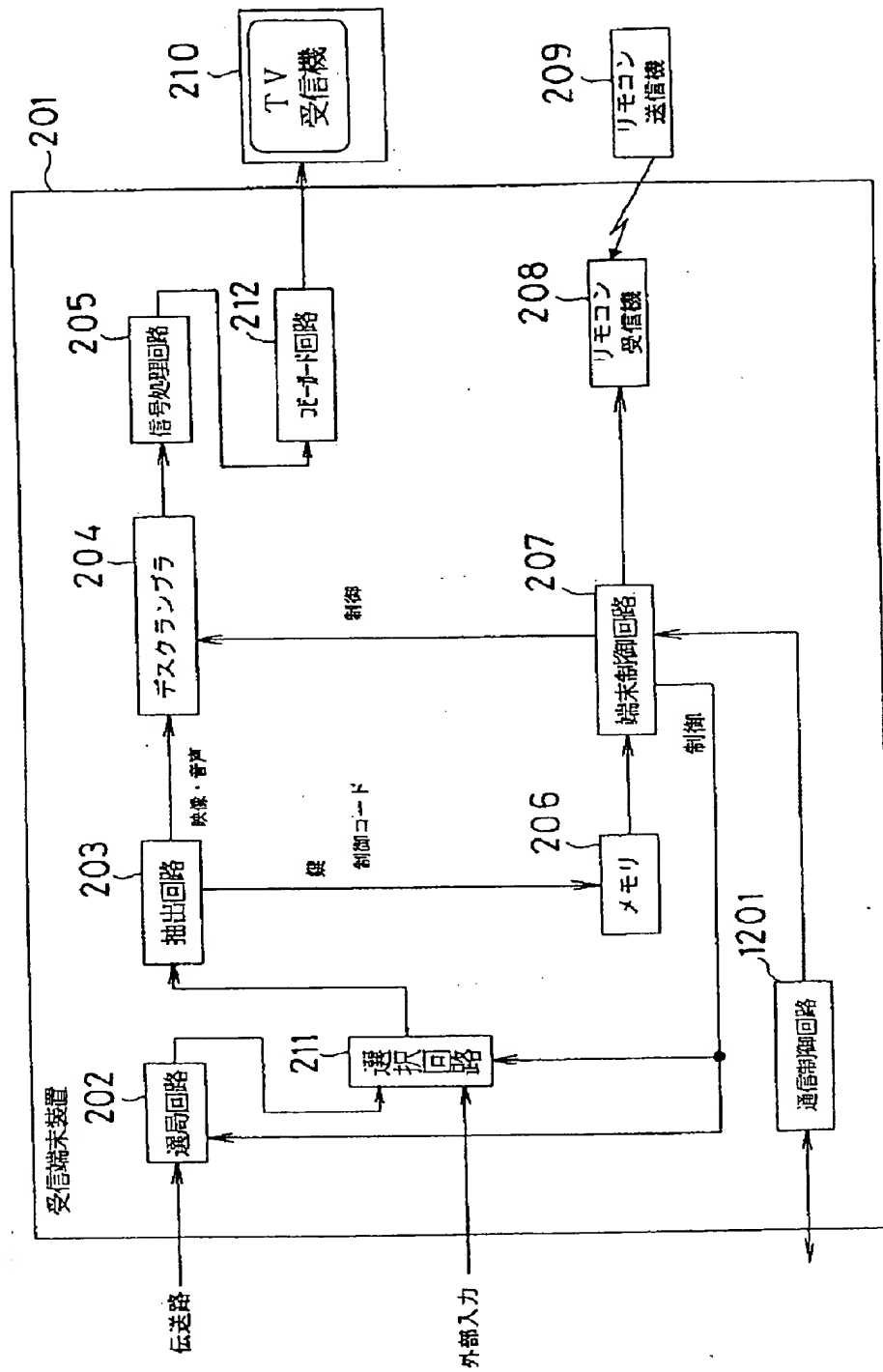
【図 11】



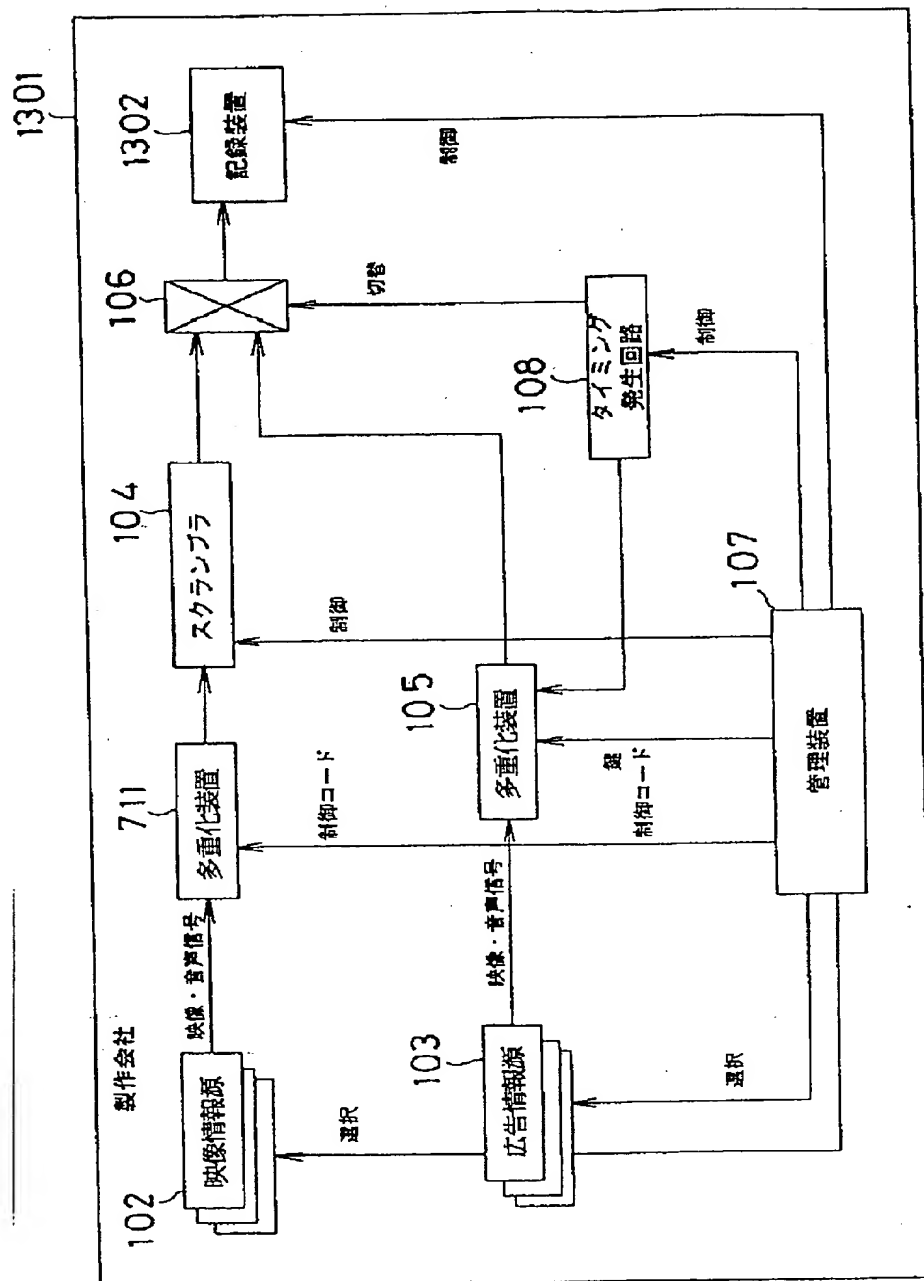
【図 12】



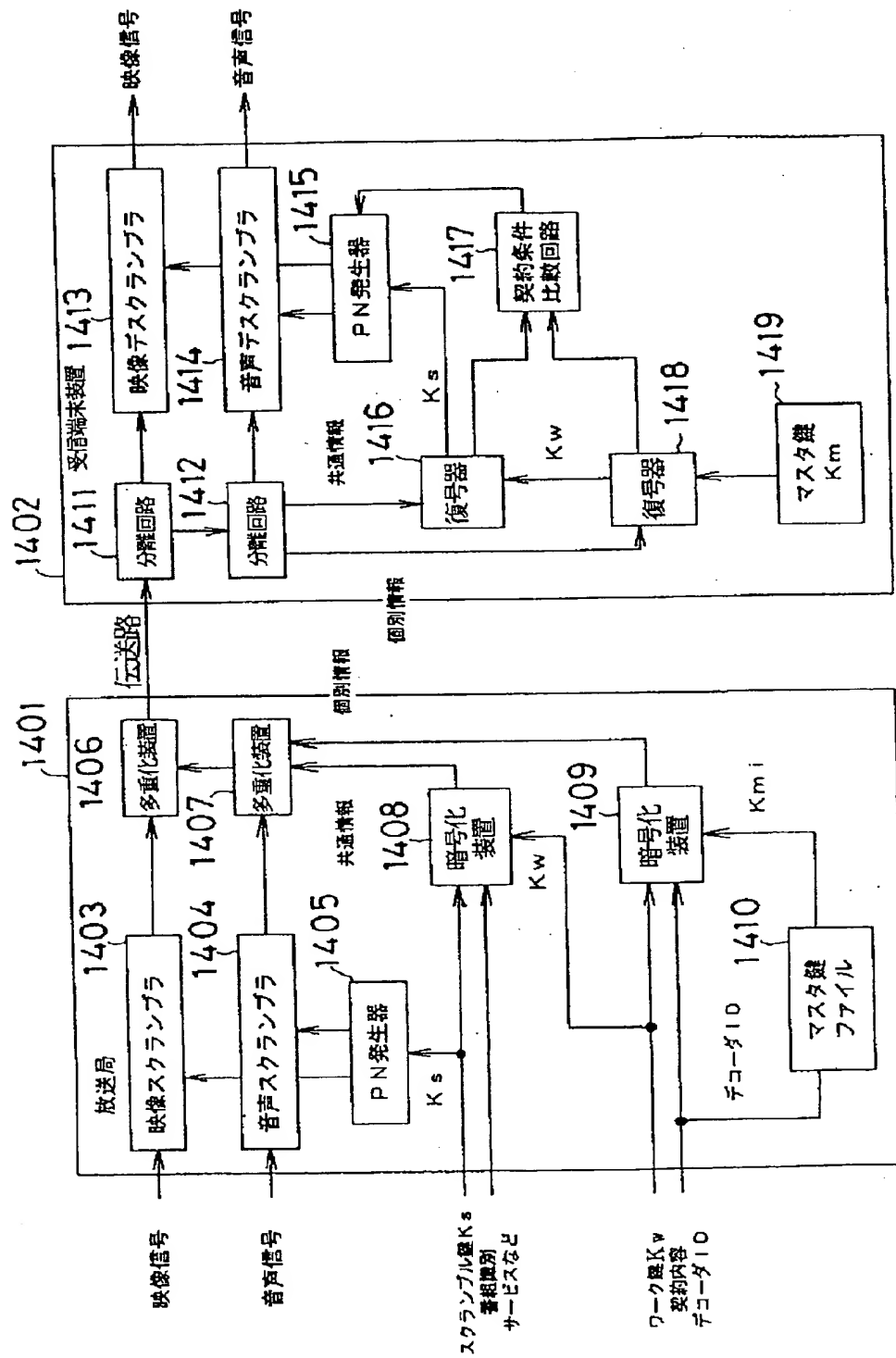
【図 13】



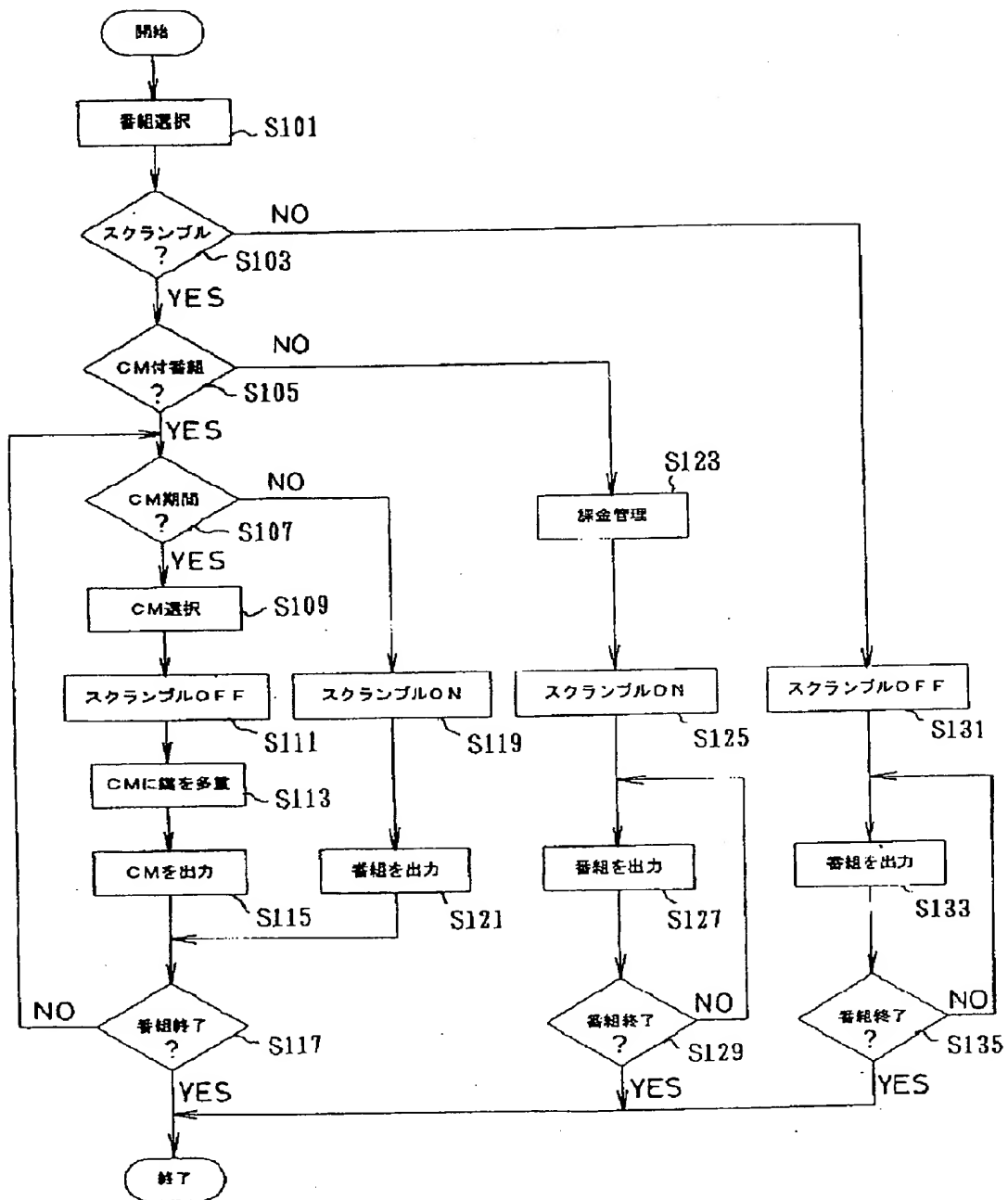
【図 14】



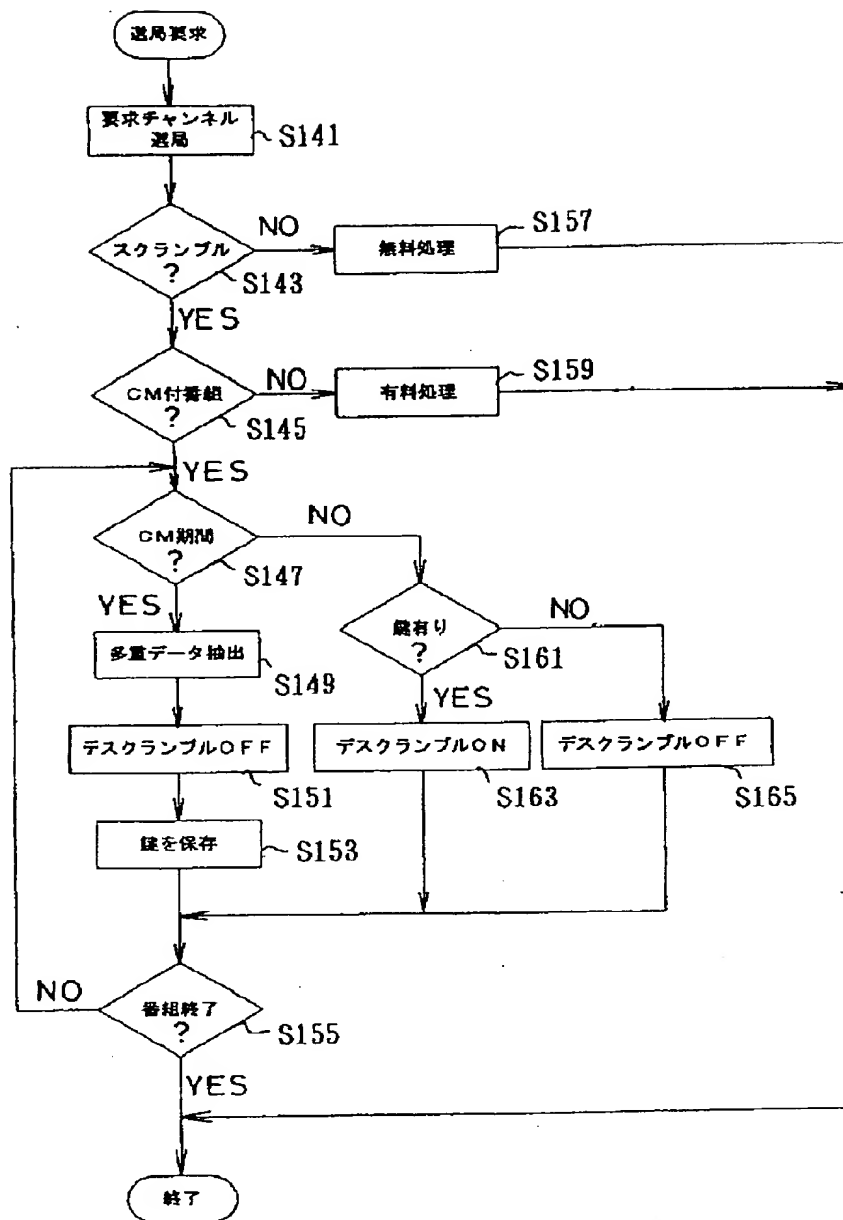
【図 15】



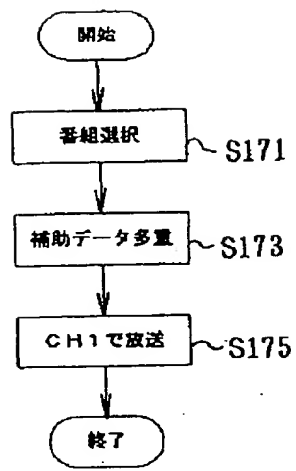
【図 16】



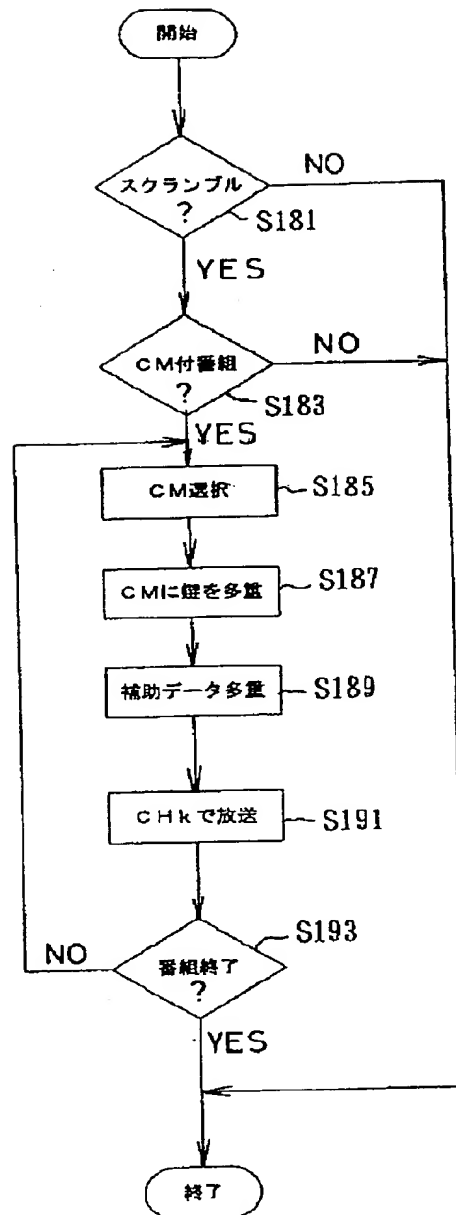
【図 17】



【図 18】

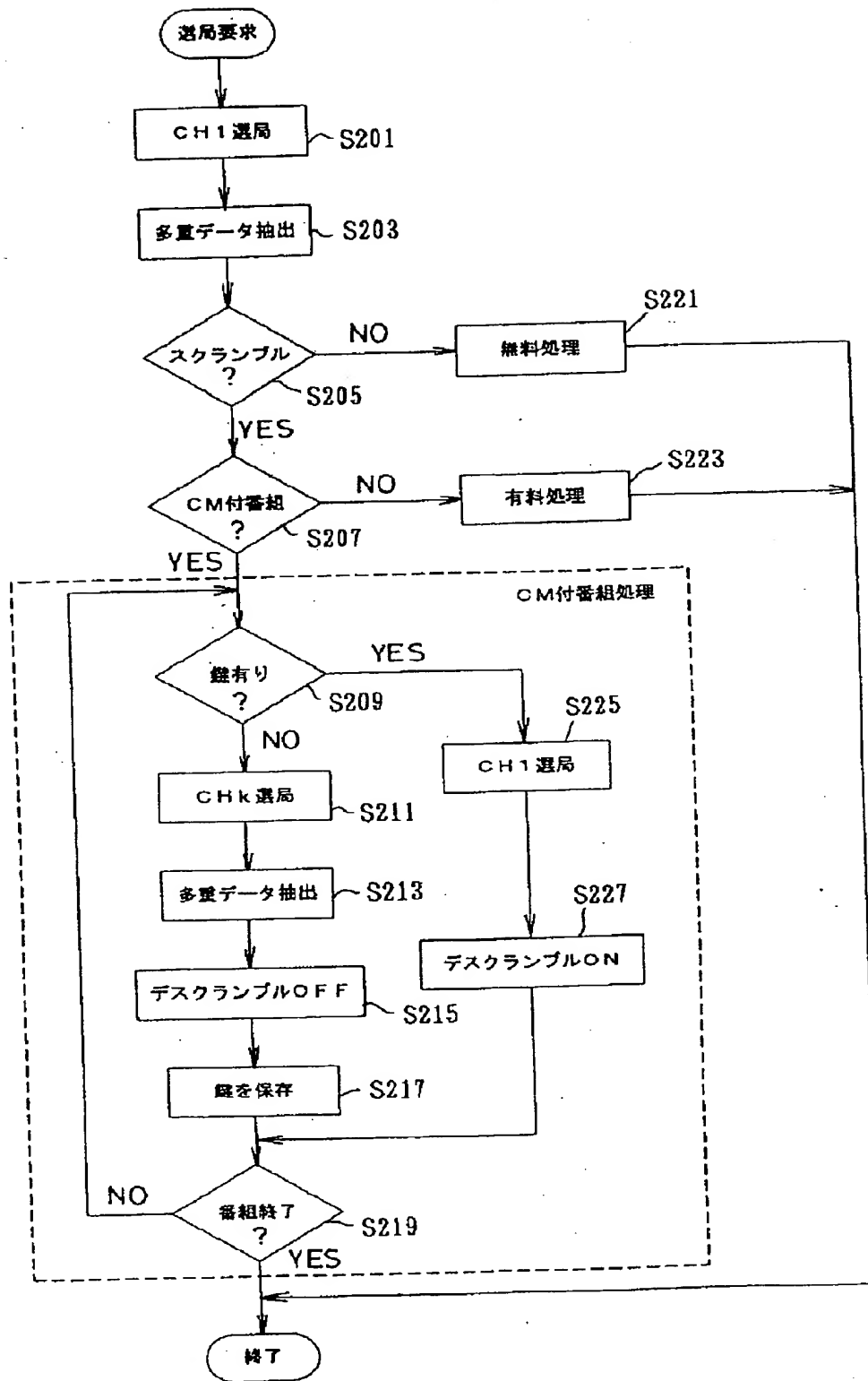


(a)

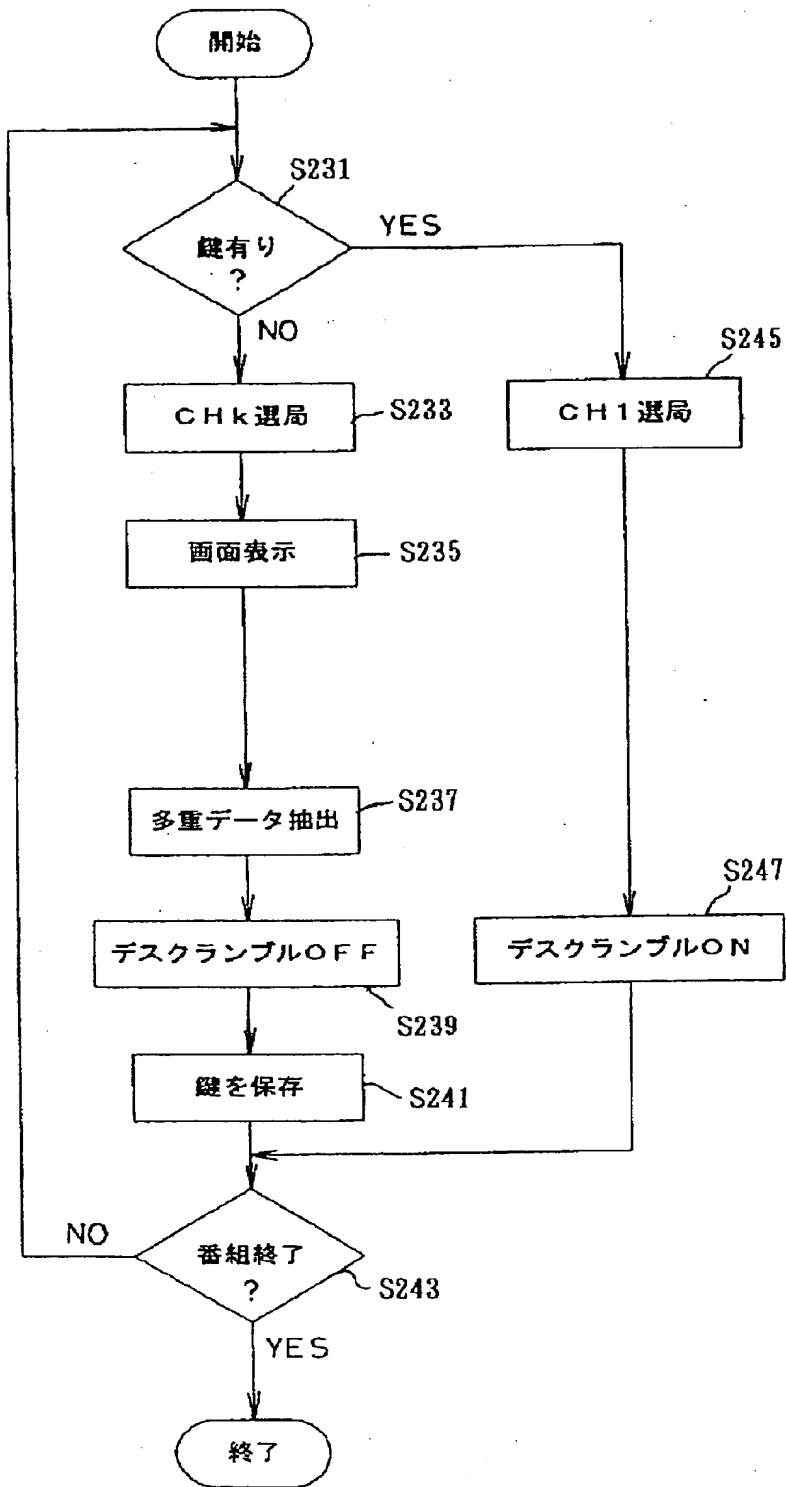


(b)

【図19】



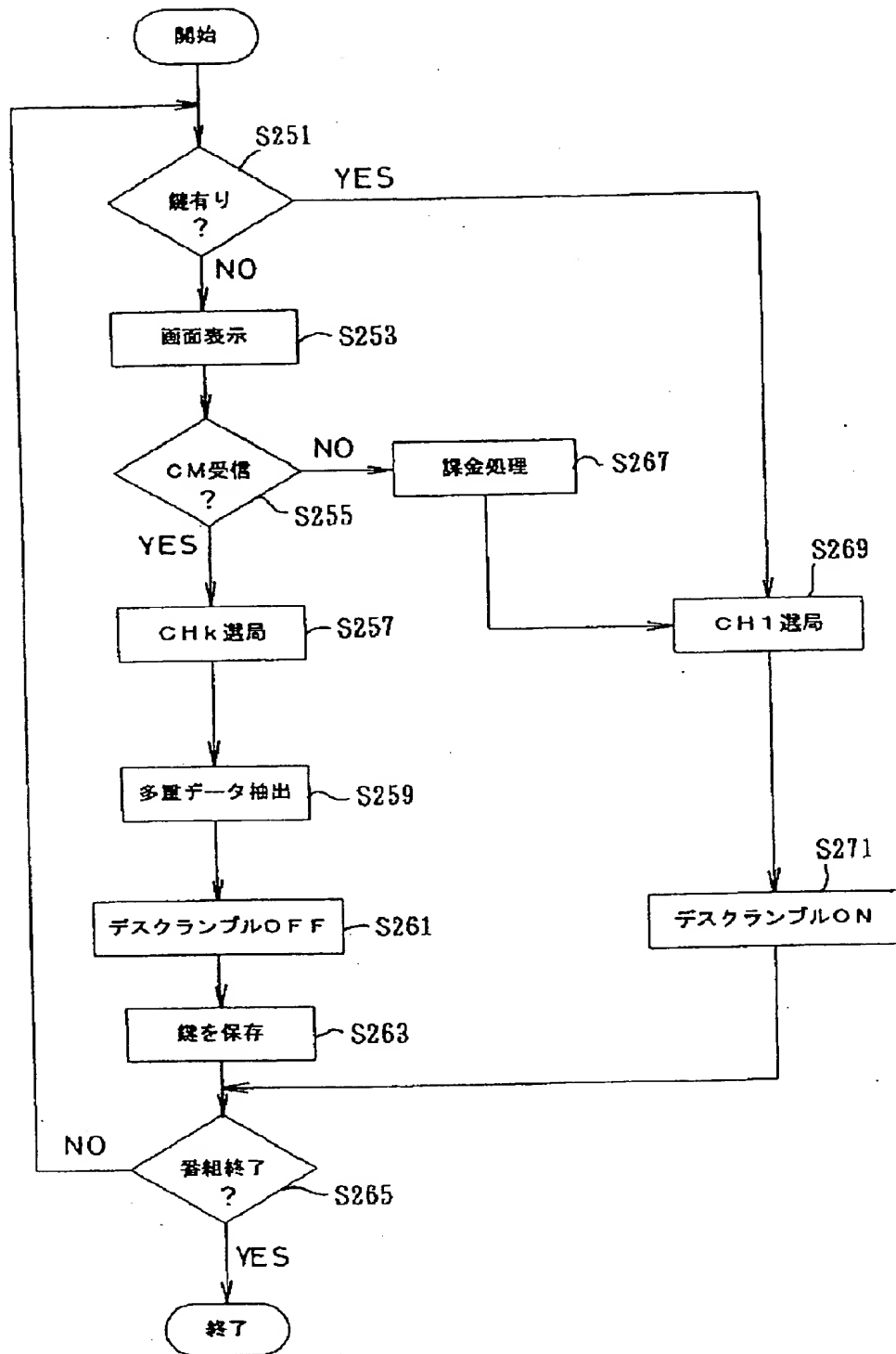
【図20】



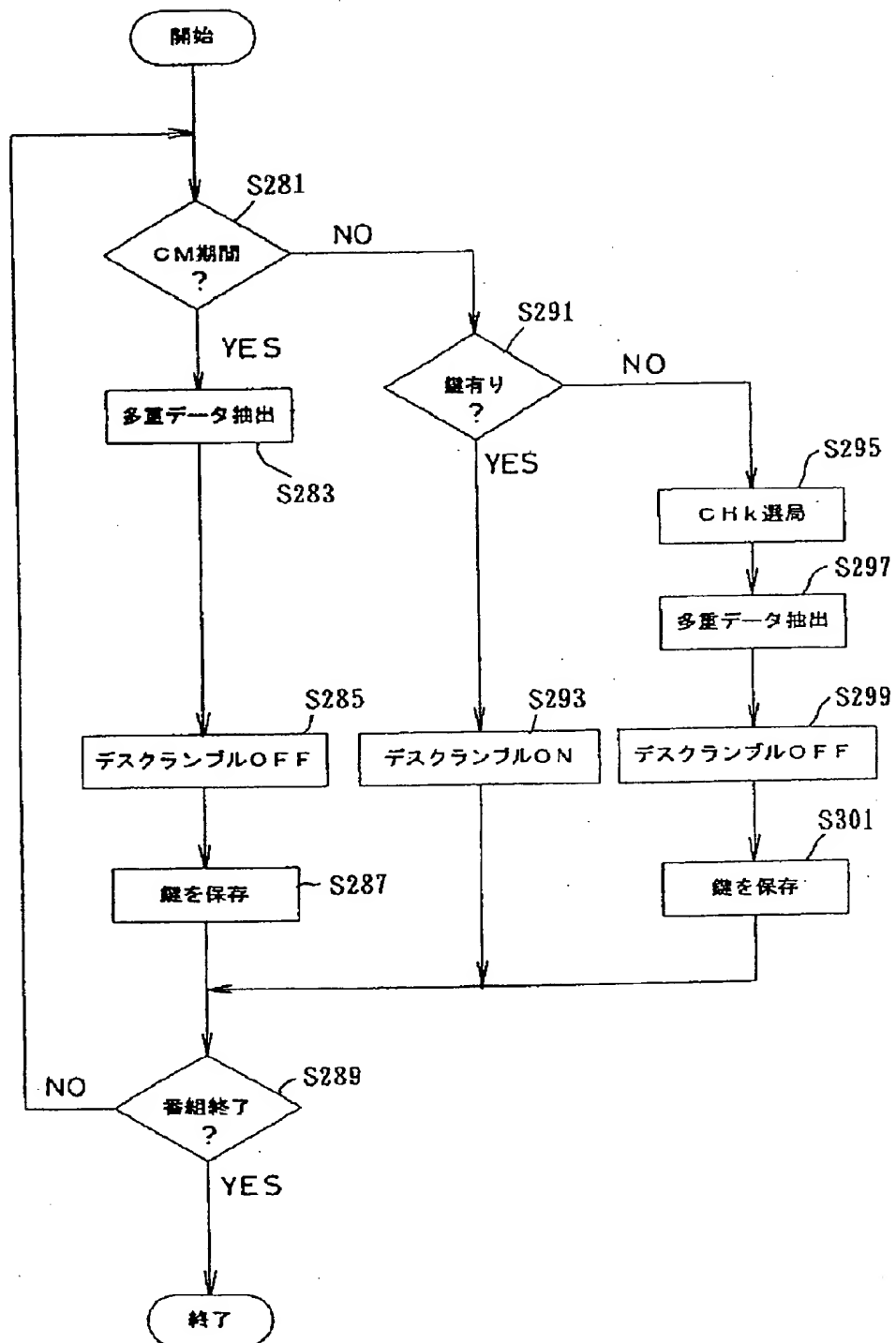
【図29】

CM1	鍵1	更新日時
CM2	鍵2	更新日時
⋮		
CMn	鍵n	更新日時

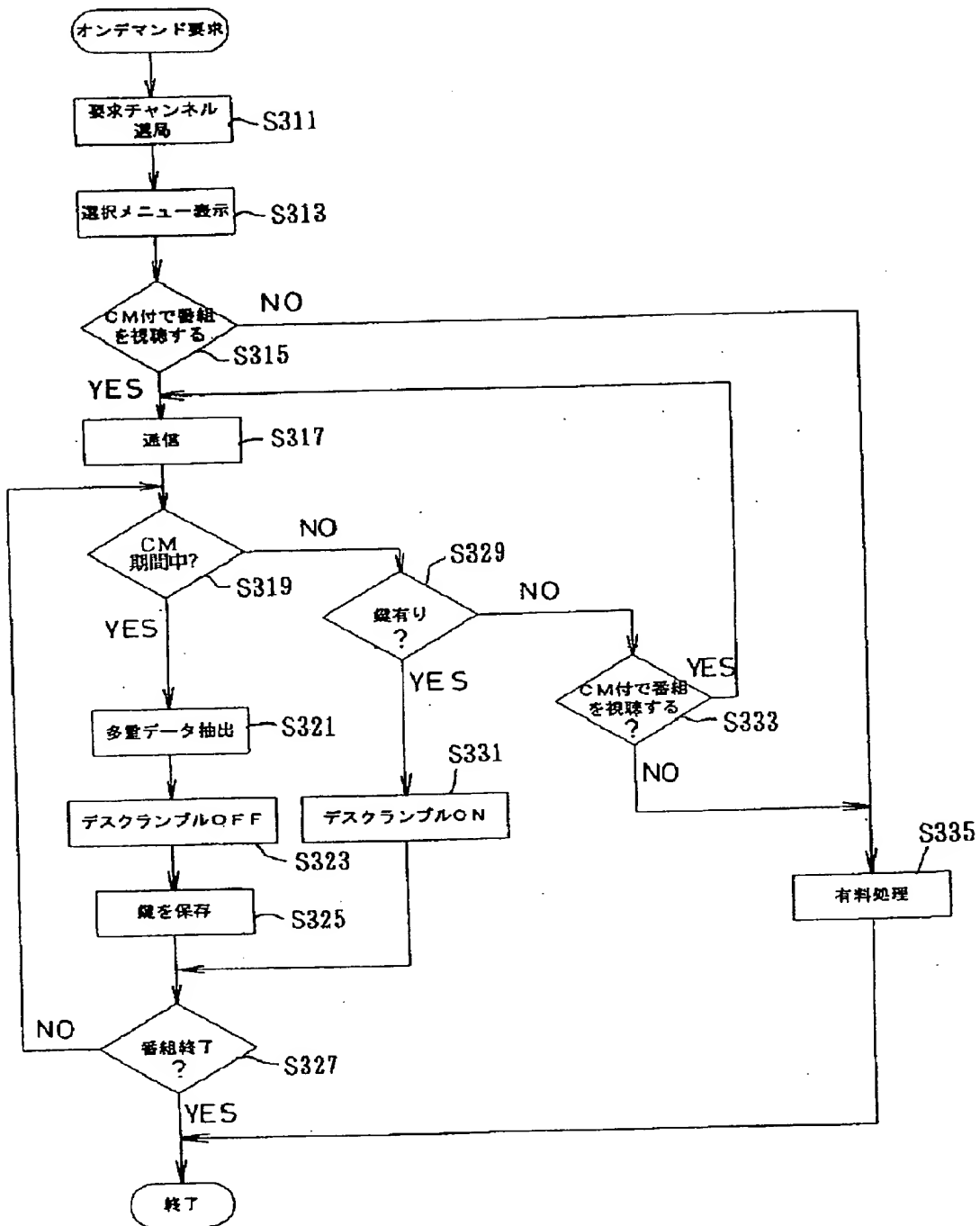
【図 21】



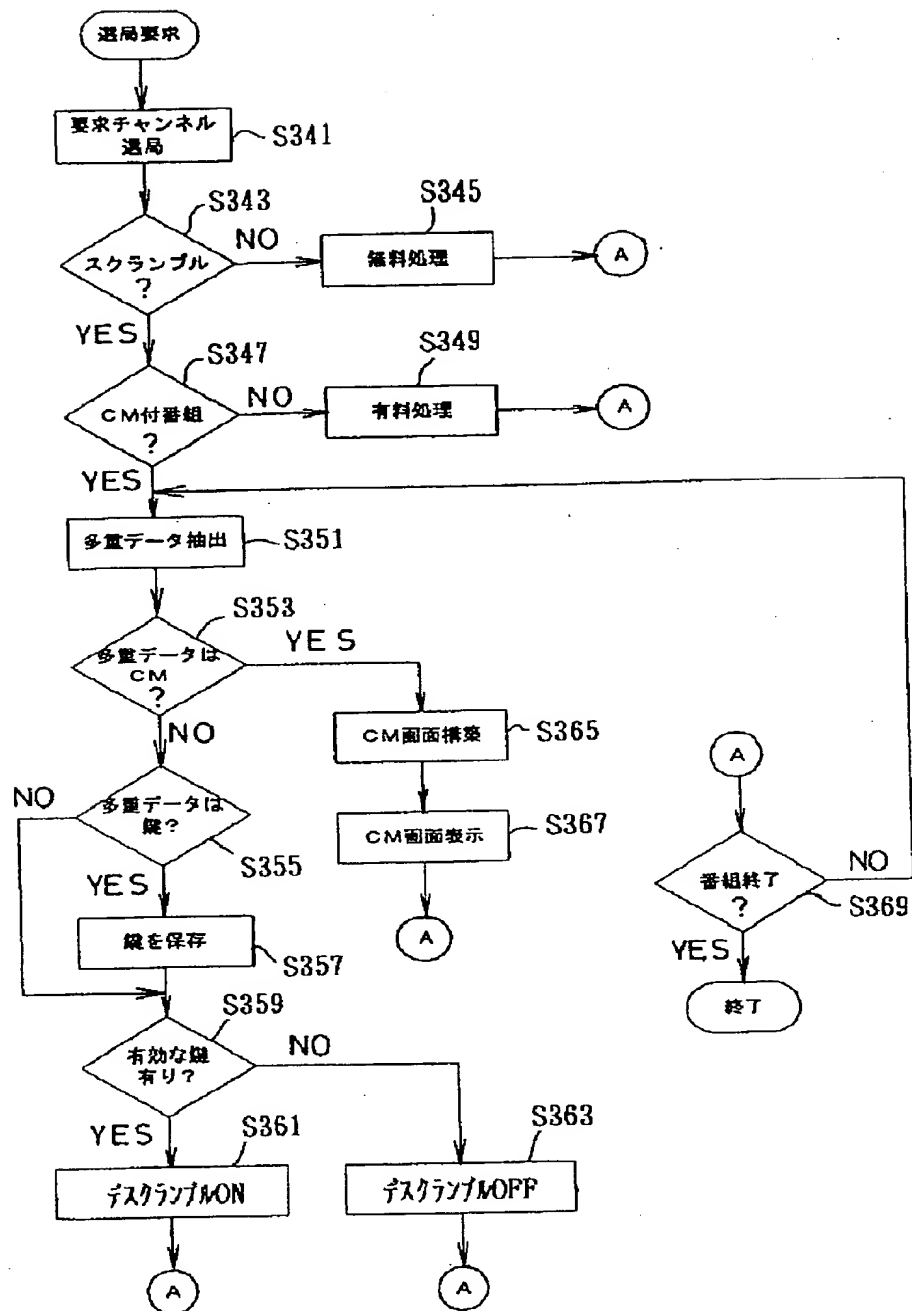
【図 22】



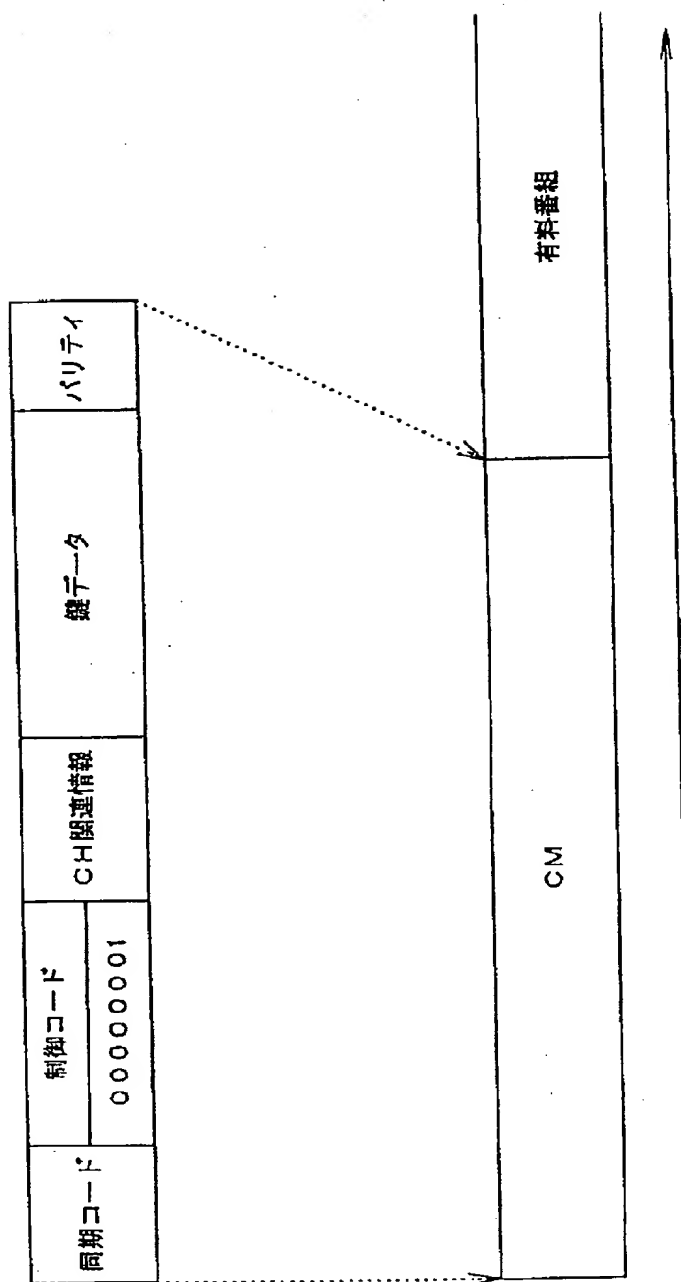
【図23】



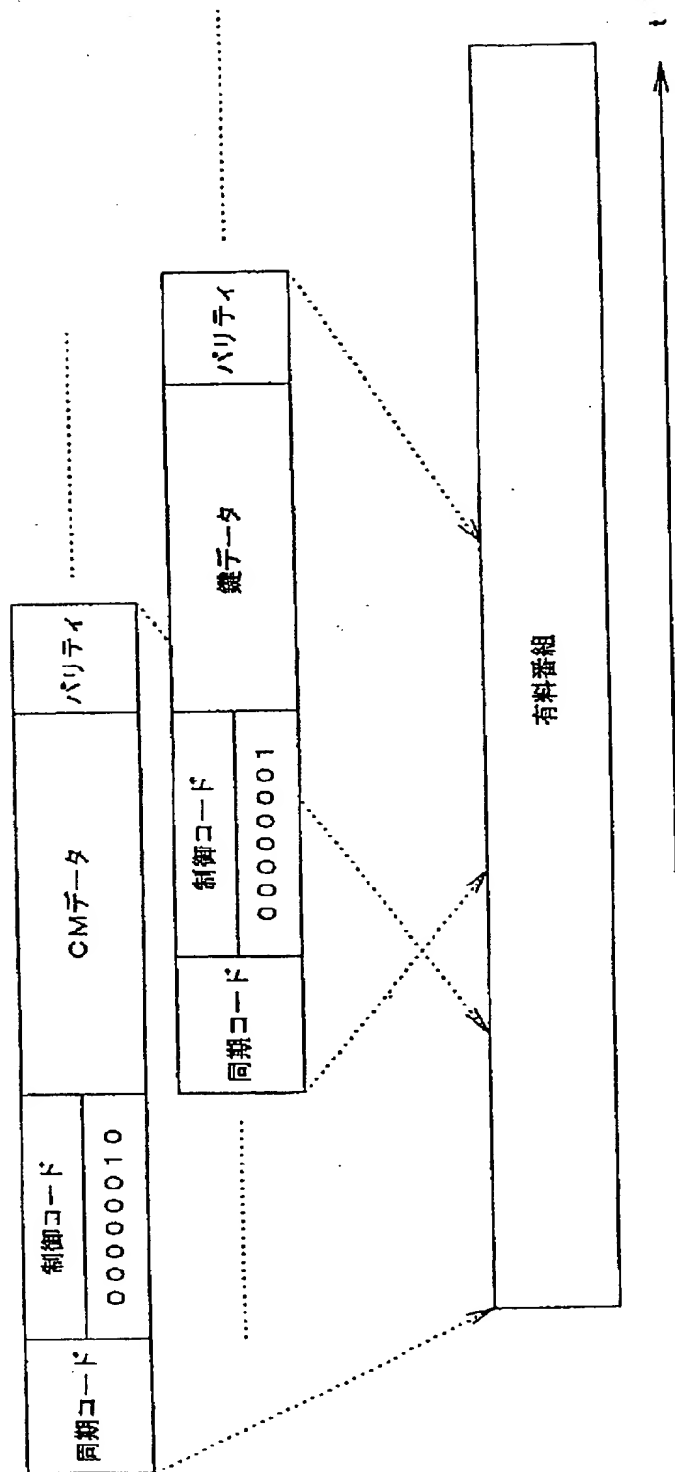
【図 24】



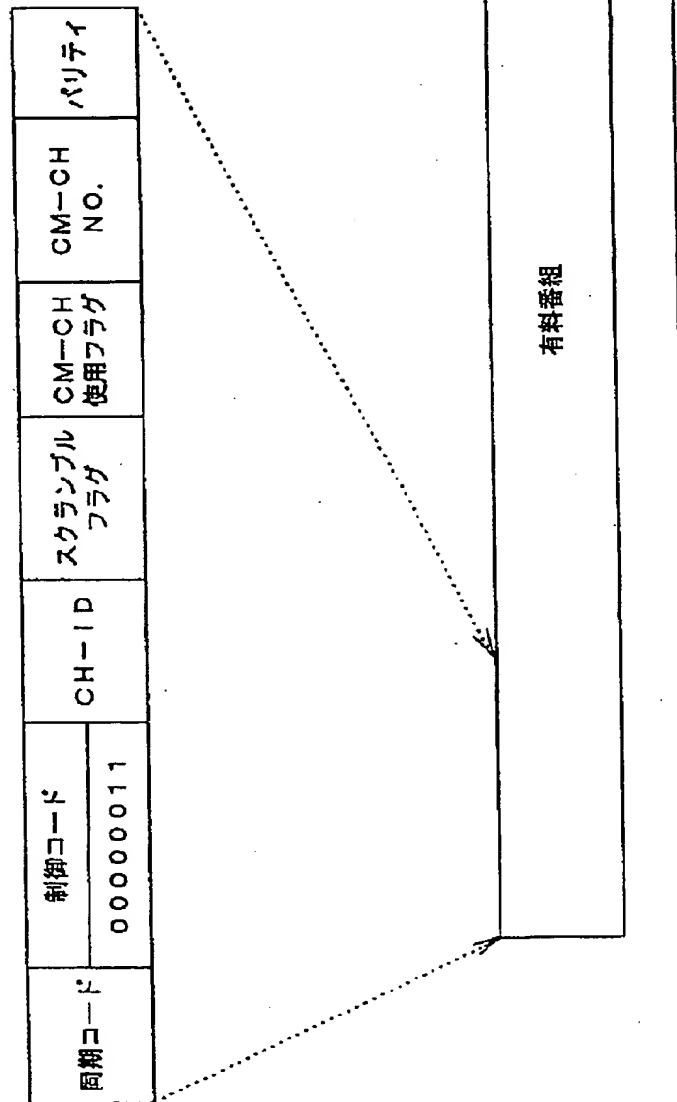
【図 2 5】



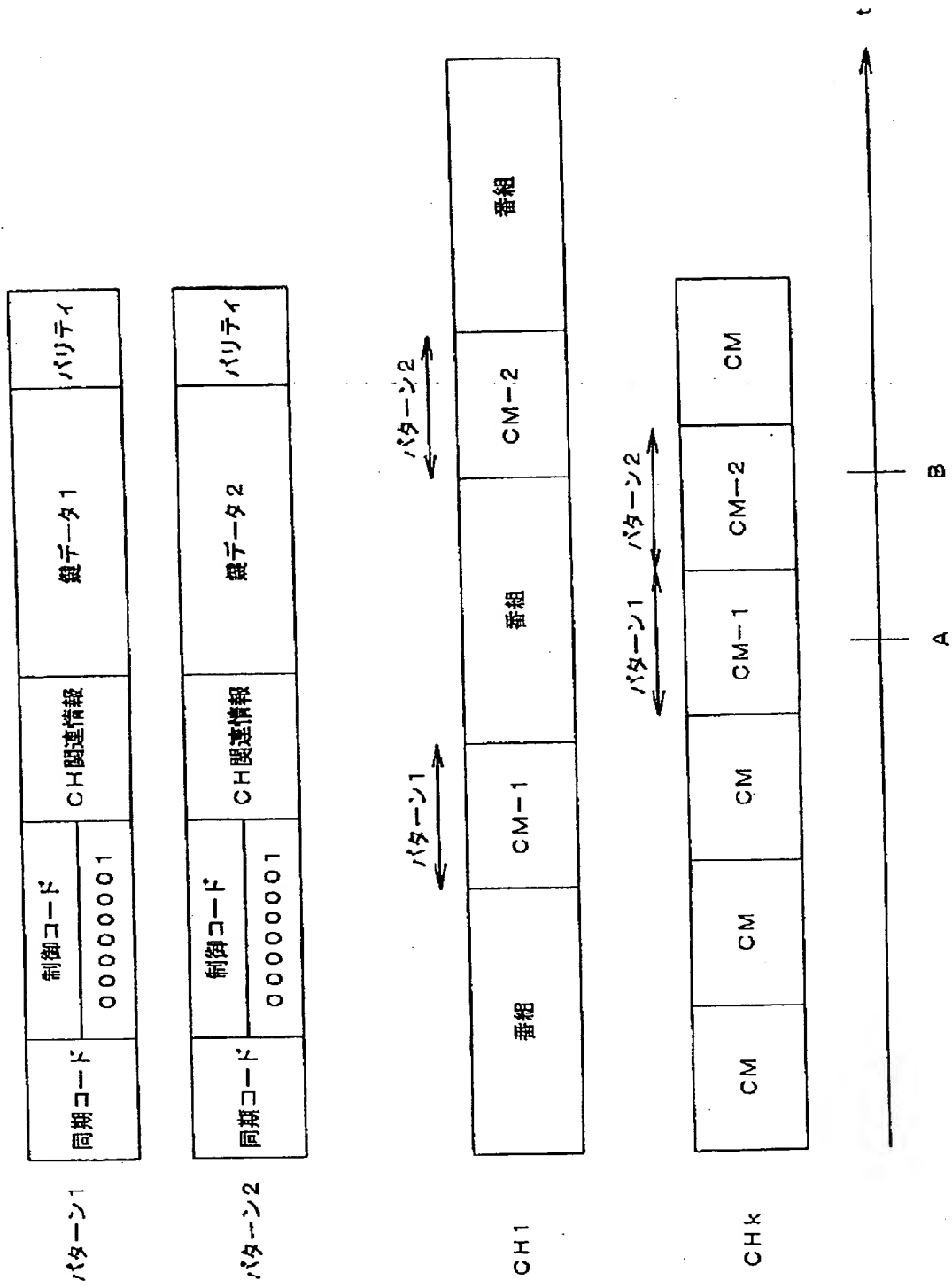
【図 2 6】



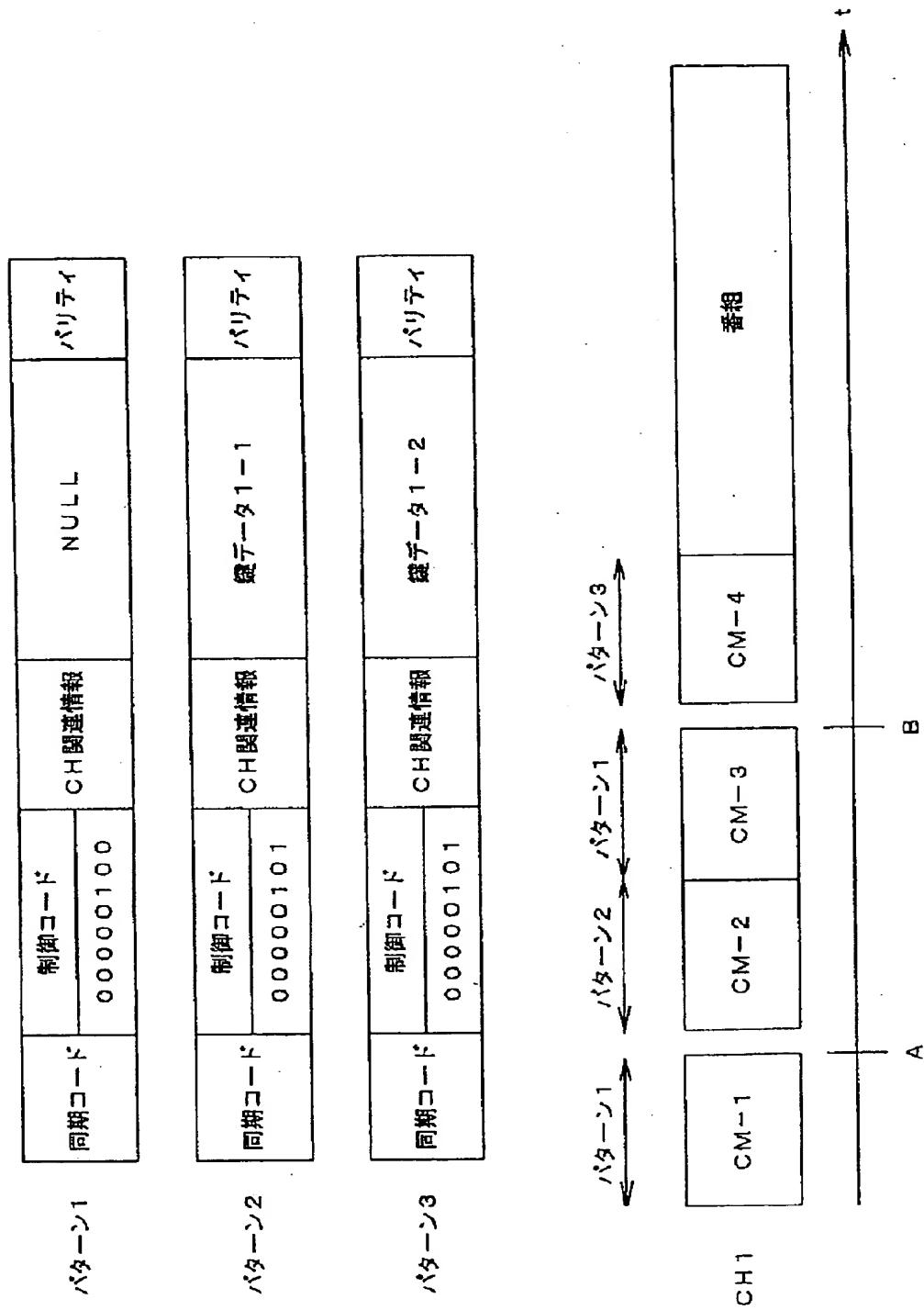
【図 27】



【図 3 0】



【図 31】



【図32】

コード	内容
00000001	鍵を多重している。
00000010	CMデータを多重している。
00000011	チャンネル識別コード等を多重している。
00000100	多重データはない。
00000101	鍵を分割して多重している。
00000110	予備
11111111	予備

【図33】

ビデオオンデマンドメニュー

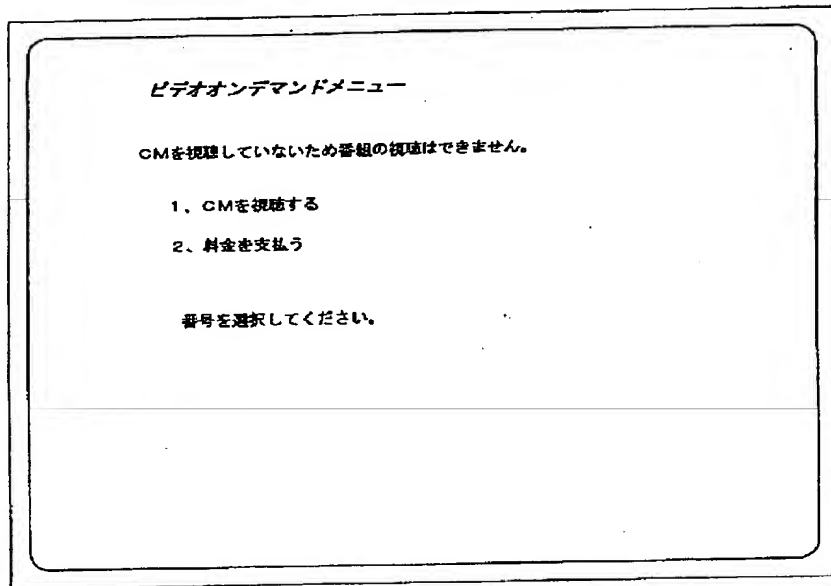
ただいま放送可能な番組は以下の番組です。

1、番組101	800円 (CM付200円)
2、番組102	500円 (CM付200円)
3、番組103	800円 (CM付無料)

番号を選択してください。

CM付であれば'1'、なしの場合は'2'を入力してください

【図34】



LIST OF THE RELEVANT PRIOR DOCUMENT

1. "A Capsulated Content Distribution Architecture (1) - Total structure & adaptive content services -" by Itaru Hosomi, Masayuki Nakae, Shunji Ichiyama, October 5 to 7, 1998, pp. 3-13 to 3-14, Collected papers of Lecture (3); The 57th National Convention of Information Processing Society of Japan
2. "A Capsulated Content Distribution Architecture (2) - On Demand Access Control with Tickets -" by Itaru Hosomi, Masayuki Nakae, Shunji Ichiyama, October 5 to 7, 1998, pp. 3-15 to 3-16, Collected papers of Lecture (3); The 57th National Convention of Information Processing Society of Japan

RELEVANT PART

1. "A Capsulated Content Distribution Architecture (1) - Total structure & adaptive content services -"

In the face of distribution of digital content as articles for sale, as its main problem, there is an unauthorized use of the articles based on the easiness of the digital content duplication. There are two ways to approach this problem: one is a copy protection and a restriction of access for preventing such unauthorized copies; and the other is a capsulation (encryption) to render the content unavailable without a specific procedure, meanwhile the content duplication is free. This article describes a content distribution architecture making a flexible use and a charging control possible, and a technique for presenting a content corresponding to the demand of users and an environment for the usage as its characteristic, on adoption of the capsulation.

"MediaShell" makes restructure matters displayed on the same content in accordance with a terminal and a request, after capsulation, so that the content can be used more pleasant. In addition, since each of elemental objects displayed as a result of the restructure is individually managed in a capsule of the MediaShell, the charge

corresponding to the displayed content can be possible in the same content.

2. "A Capsulated Content Distribution Architecture (2) - On Demand Access Control with Tickets -"

There will be described a usage/charge control system on a capsulated content distribution architecture which is described in another article. In this system, the usage/charge control is performed by selling a permission (ticket) for the usage of the content.

The characteristic of this system is in a point of the setting of the usage condition and the charge condition every structural elements of the content, and allows a further flexible usage/charge control in comparison with the conventional system. The usage condition and the charge condition in every structural elements are described by using an access control list (ACL). The margin of safety for the capsulated content can be realized by managing in a reliable ticket server with the separation of the ACL.

This distribution system realized highly safety usage control by using the following ideas: (1) encryption by an object key which is different every elemental objects; (2) transaction of a ticket key relied on not the transaction of the object key but the usage; and (3) reproduction of the object key by only the combination of an adequate ticket key and the usage key.

In addition, this distribution system improved the flexibility and safeness of the usage condition by using the following ideas: (1) description by means of not the unit of content but the unit of the object and usage; and (2) delegation of management to the reliable ticket server with separation of ACL from the content.

第57回(平成10年後期)全国大会

講演論文集(3)

データベースとメディア

データベース

情報検索

メディアと情報

ネットワーク

マルチメディア通信と分散処理

分散システム運用

マルチメディア符号化

モバイルコンピューティング



平成10年10月5日～7日 於：名古屋大学

 社団法人 情報処理学会

Information Processing Society of Japan

カプセル化コンテンツ流通基盤(1) - 全体構成と利用状況適応機能 -

1 K-7

細見 格 中江 政行 市山 俊治

NECヒューマンメディア研究所

1. はじめに

商品としてのデジタルコンテンツの流通を考えた場合、その主な問題としてデジタルコンテンツの複製の容易さに基づく商品の不正使用が挙げられる。この問題への対処法には大きく二種類あり、一方はコンテンツの無断複製を防ぐコピープロテクトやアクセス制限、もう一方は複製自体は自由だが特定の手続き無しにはコンテンツを利用できなくするカプセル化(暗号化)である。本稿では、カプセル化を採用した上で柔軟な利用と課金制御を可能にしたコンテンツ流通基盤、およびその特徴として利用者の要求や利用環境に応じた内容を提供する技術について述べる。

2. カプセル化コンテンツ流通基盤

本研究では、コンテンツのカプセル化アーキテクチャとして MediaShell [1] を採用したコンテンツ流通基盤を構築している。本研究のコンテンツ流通モデルは図1のような構成となっている。

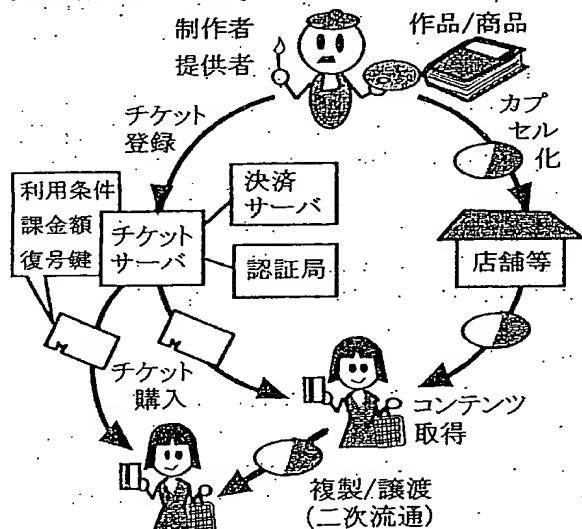


図1 カプセル化コンテンツ流通モデル

図1でチケットとは、ある特定のコンテンツの価格と利用条件、およびそのコンテンツを復号するための鍵を含む暗号データである。デジタルコンテンツは複製が容易な上、同じコンテンツでも利用時の端末装置や利用者の要求は様々である。そこで本研究では、利用者が適

*A Capsulated Content Distribution Architecture (1)
- Total structure & adaptive content services -
Itaru Hosomi, Masayuki Nakae, Shunji Ichiyama
Human Media Labs., NEC Corp.*

当なチケットを選択して購入することにより、同じコンテンツでも用途に適した品質や構成で内容を得られ、それらに応じた支払いを行なうことができるようにしている。また、本研究では得られたコンテンツを各状況下で快適に利用できるようにするために、利用状況適応機能を前述の MediaShell の機能として実装した。なお、利用と課金の制御については別稿 [2] で詳述している。

3. デジタル情報コンテンツ MediaShell

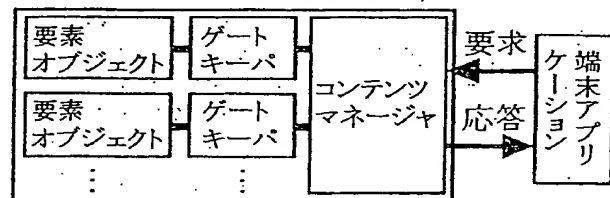
3.1 カプセル化コンテンツとコンテナ

コンテンツをカプセル化したものをカプセル化コンテンツまたは単にカプセルと呼び、1つのカプセルに納められる要素の種類や構成を定義したものをコンテナと呼ぶ。カプセルはそれ自体の安全性が高いため自由な経路で流通させることができるが、反面、コンテンツを利用できる環境や表現形態への制限が多い。本研究では、コンテンツの安全性と利用の柔軟性を両立させたカプセルを実現するデジタル情報コンテンツ MediaShell を提案し、その開発を進めている [1]。

3.2 MediaShell アーキテクチャ

本流通システムのベースとなる MediaShell の基本構造については先の論文[1]で述べた。MediaShell 形式のカプセルは、コンテンツマネージャ、ゲートキーパおよび各ゲートキーパが管理する要素オブジェクト群からなる(図2)。既存技術との主な違いは以下のような点である。

1. 要素オブジェクトの構成を管理だけでなく、要求に応じて出力時の構成変更が可能。
2. 各要素オブジェクトの役割やコンテンツ制作者の意向を考慮した上記構成変更処理の制御が可能。



MediaShell カプセル

図2 MediaShell の基本構造

4. コンテンツの利用状況への適応

2章で述べたようにデジタルコンテンツの利用状況は多種多様であり、各状況において可能な限り効果的にコンテンツを提供する技術は、利用者/提供者双方にとつ

て重要である。Media-Shellは要素オブジェクトを個別に管理し、その構成を木構造で保持・制御することにより図3に示すような各種の利用状況適応機能を実現している。以降では論文[1]で述べていないレイアウト変更機能と部分要素抽出機能について説明する。

要素縮小表示	代替要素提供
要素表示オンデマンド化	レイアウト変更
出力不可要素削除	部分要素抽出

図3 MediaShell の利用状況適応機能一覧

4.1 オブジェクト構造の木構造化

MediaShell は、要素オブジェクトの表示画面上の構成を木構造で表現し、汎用的なルールを用いて構成を変更することにより、以下のような要求にも対応できる。

- ・未知の解像度／縦横比の端末画面への自動適応
 - ・要素オブジェクト間の隣接関係や包含関係の維持
- 木構造は画面上の領域分割をノードの分岐に対応させ、以下のように表現している。

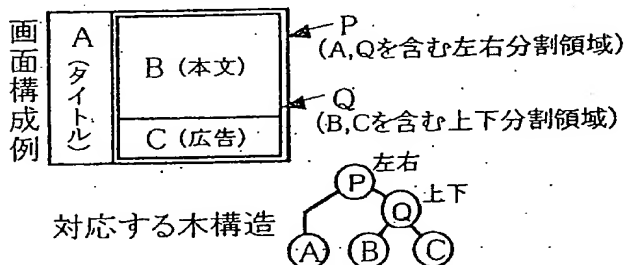


図4 コンテンツの出力画面構成例と対応する木構造

4.2 レイアウト変更機能

端末の制約や利用者の要求は以下のようなスクリプトで表現し、カプセルにメッセージとして送る。

例: play adaptive
condition client.disp.width = "640"
and client.disp.height = "480"; (1)

これに対して、カプセル内には適応表示用のルールを例えば次のように記述する。

- 1: cond="client.disp.height < profile.disp.height"
// 条件: 端末画面の高さが必要解像度未満なら、
 - 2: ope="horizontal gk03.ad" // 広告を90度配置変更
 - 3: ope="reduce gk01.title" // タイトルを簡略表示
- カプセル外部から受け取ったメッセージ(1)とカプセル内部のルール(2)から、コンテンツマネージャが要素オブジェクトの構成を表す木構造を変更する。

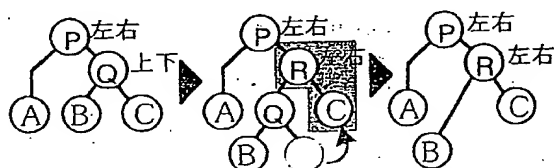


図5 ルール(2)と図4の例に基づく変更処理

ルール(2)で cond="..." を条件、ope="..." をメソッドと呼ぶ。図5はルール(2)の 2: で示した horizontal メソッドを実行した場合の処理である。このメソッドは、変更対象の表示要素と隣接する要素との位置関係を上下から左右に変更する。結果として、図6右側のように表示領域の高さの不足に対処したレイアウトとなる。ここで領域AやCの高さは許容範囲内で自動調整され、許容最小サイズを超える場合はルール中の次のメソッドを適用する。条件を満たすかメソッドが尽きれば、そのルールの参照を終える。

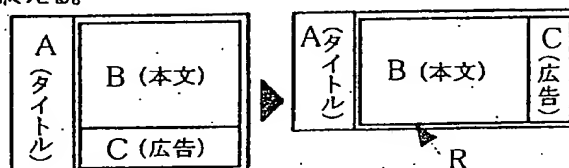


図6 レイアウト変更結果

このような木構造への部分木挿入やノード付替えにより、配置の変更を行なっても要素オブジェクト間の隣接関係や包含関係(木構造のノードの親子関係)が自動的に維持されるため、例えばメニューとその選択結果の表示領域との対応が崩れるのを防ぐことができる。

4.3 部分要素抽出機能

MediaShellでは下記の例のようなメッセージによりコンテンツ内の希望する部分のみを抽出することができる。

例: select *title // タイトルを検索
condition client.disp.imageout = "no" // 画像不可
where date >="19980716" // 制作日条件指定
and format = "html"; // ファイル形式は HTML

上記の例では検索条件(where)の他に前記(1)と同様の出力条件(condition)がある。検索条件を満たしても出力条件を満たさない要素は前節と同様に可能ならば適応化処理を施し、不可能ならばその由を示す。

5. おわりに

以上のような機能により、MediaShell ではコンテンツをカプセル化した上で同じコンテンツでも表示される内容を端末や要求内容に応じて再構成できるため、コンテンツをより快適に利用できる。また、再構成した結果として表示される各要素オブジェクトを個別に MediaShell のカプセル内で管理しているため、同じコンテンツに対して表示内容に応じた課金も可能である[2]。

参考文献

- [1] 細見, 他: 多様な再生環境に適応する流通コンテンツ・アーキテクチャの提案, 情報処理学会第55回全国大会論文集, 6Q-05, 1997.
- [2] 中江, 他: カプセル化コンテンツ流通基盤(2)-チケットによる利用制御方式-, 情報処理学会第57回全国大会論文集, 1K-08, 1998.

カプセル化コンテンツ流通基盤(2)

-チケットによる利用制御方式-

中江政行 細見格 市山俊治

NEC ヒューマンメディア研究所

1K-8

1 はじめに

別稿[1]で述べたカプセル化コンテンツ流通基盤における利用/課金制御方式について述べる。本方式では、コンテンツの利用許可証(チケット)の販売により利用/課金制御を行う。

本方式の特徴は、コンテンツの構成要素ごとに利用条件と課金条件を設定できる点にあり、従来方式に比べ、より柔軟な利用/課金制御を可能にする。構成要素ごとの利用条件および課金条件は、アクセスコントロールリスト(ACL)を用いて記述される。ACLをカプセルから分離し信頼できるチケットサーバで管理することで、カプセル化コンテンツの高い安全性を実現できる。

本稿では、コンテンツのカプセル化形式と、チケット方式によるコンテンツ利用制御機構について述べる。

2 コンテンツ流通システム

本システムは、コンテンツ視聴に用いる「ビューワ」、エディタ等で作成されたコンテンツのカプセル化を行う「カプセルジェネレータ」、ACL管理とチケット配信を行う「チケットサーバ」、利用料金の振込処理を行う「決済サーバ」、カプセル化されたコンテンツデータとその操作メソッドから成る「MediaShell コンテナ」から構成される(図1)。

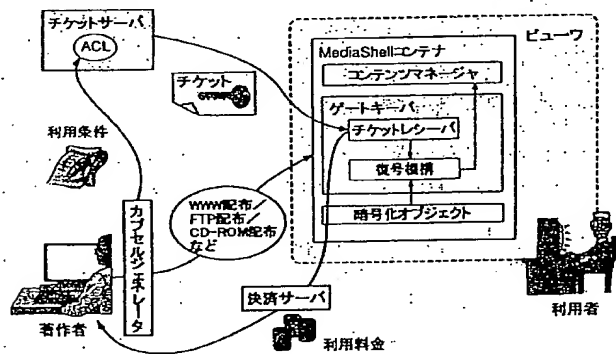


図1: システム構成

3 MediaShell コンテナ

MediaShellは我々が提案するマルチメディアコンテンツカプセル化技術であり、コンテンツの構成要素ごとの

利用/課金制御などを特徴とする[1][2]。

利用/課金制御の対象を「(要素)オブジェクト」と呼ぶ。オブジェクトとして何を選ぶかは、コンテンツの性格によるが、例えばWWWコンテンツの場合、1つのhtmlファイルもしくは1つの埋め込みデータ(画像ファイル/動画ファイル等)とすることができる。

MediaShell コンテナは、以下のような構造をもつ。

- MediaShell コンテナは、各オブジェクトに対応した複数のゲートキーバと、それらを束ねる1つのコンテンツマネージャをもつ。
- コンテンツマネージャはゲートキーバへのオブジェクトデータ要求を行い、表示イメージの生成を行う。
- ゲートキーバは1つの暗号化オブジェクトデータと関連づけられており、チケット要求/受信を行うチケットレシーバとオブジェクトデータ復号を行う復号機構により、コンテンツマネージャへのオブジェクトデータ出力を制御する。

各ゲートキーバがもつ復号機構では、関連づけられた暗号化オブジェクトに関する以下のような情報が保持されている。

- 著作権情報(著作者名, 作成日時, オブジェクト名など)
- 利用鍵テーブル(利用法/利用鍵)

利用鍵は、それぞれ一つの利用法に対応づけられている。利用法 U に対応する利用鍵 K_U は、一方向性ハッシュ関数 $hash$ を用いて $K_U = hash(\text{著作権情報}|U)$ と表される。

暗号化オブジェクトデータは、慣用暗号により暗号化されたオブジェクトデータである。その際に用いられる鍵は乱数により決定される。この鍵をオブジェクト鍵(K_{obj})と呼ぶ。

4 利用制御方式

4.1 チケット方式

MediaShell コンテナは、任意のftp サイトやWWW サイトを通じて、自由に配送される。そして、利用者がコンテナ内のコンテンツを利用する際に、その旨をチケットサーバに要求し、特定のチケットを取得してはじめて利用できる仕組みになっている。一方、チケットサーバは、利用者からの要求と要求対象であるコンテンツの利用条件とを照合し、条件に合致する要求に対してのみ適切なチケットを生成/配信する。

チケットによる利用制御方式は、以下のような特徴をもつ。

- 従来コンテナ内に同梱されていた利用条件を、信頼できるチケットサーバに管理させることで、より高い安全性を実現できる。
- 利用条件をオブジェクトおよび利用方法ごとに記述できるようにすることで、利用制御の柔軟性を向上させることができる。例えば、オブジェクトごとにペイパービュー/時間課金など、異なる課金方法を選択できる。
- チケット鍵分割により、二次著作物の著作権保護および流通を可能とする。

以下の項では、柔軟な利用条件記述を可能にする ACL について説明し、チケット送受とコンテンツ利用について説明する。

4.2 ACL

ACLでは、オブジェクトごとに利用条件とチケット鍵との組を記述していく。利用条件は、例えば、

```

picture.gif {
  View {
    cond {
      Resolution <= 640x480
      ColorDepth <= 16
      Price = 3
      PaymentWay = PayPerView
    }
    key {
      9AFB38A2
    }
  }
  Print {
  }
}

```

#対象オブジェクト名
#640x480に関する条件記述
#利用条件
#解像度の上限
#色数の上限
#課金額
#課金方法
#チケット鍵定義
#印刷に関する条件記述

といったように記述される。この例において、オブジェクト picture.gif の閲覧に関する利用条件は、「表示解像度の上限を 640x480 とし、表示色数の上限を 16 とする。課金額は 3 円で、課金方法はペイパービューである。」と解釈される。

オブジェクト obj /利用法 U に対応するチケット鍵 $K_{T(obj,U)}$ は、 $K_{T(obj,U)} = \{K_{obj}\}_{K_U}$ で表される。ここで、 $\{D\}_K$ はデータ D を鍵 K で慣用暗号により暗号化することを示す。

4.3 チケット送受およびコンテンツ利用

チケット送受およびコンテンツの利用における大まかな処理の流れを図2に示す。利用者が MediaShell 形式のコンテンツのあるオブジェクトを利用する際、対応するゲートキーパは解像度や色数などの端末情報を含んだ利用要求を生成し、チケットサーバに渡す。

要求を受け取ったチケットサーバは ACL と要求とを照合して、条件が満たされた場合にのみ、以下のような構造をもつチケットを生成し、配信する。

- チケット発行者名
- 発行年月日
- 利用を許可するオブジェクト名 obj
- 許可する利用法 U
- 利用料金 (= 課金額)
- 料金支払方法 (= 課金方法)
- チケット鍵 $K_{T(obj,U)}$
- 発行者によるデジタル署名

ゲートキーパは、チケットレシーバによりチケットを受け取り、署名による正当性の検証を行った上で、チケットに含まれるチケット鍵を取り出し、復号機構へ渡す。復号機構ではチケット鍵 $K_{T(obj,U)}$ ・利用鍵 K_U ・暗号化オブジェクトデータ obj' から、次式で表される操作を行って、オブジェクトデータ obj を復元する。

$$K_{obj} = \{K_{T(obj,U)}\}_{K_U}$$

$$obj = \{obj'\}_{K_{obj}}$$

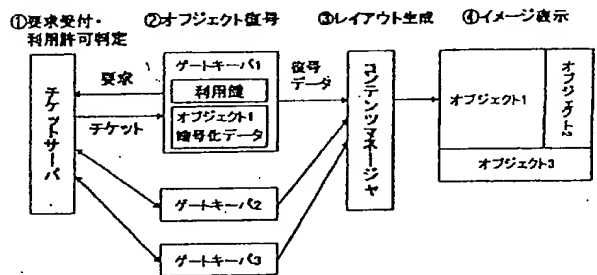


図2: チケット送受およびコンテンツ利用

5 おわりに

本流通システムでは、次のような工夫により、安全性の高い利用制御を実現した: (1) 要素オブジェクトごとに異なるオブジェクト鍵で暗号化、(2) オブジェクト鍵の取引ではなく利用法に依存したチケット鍵を取引、(3) 適切なチケット鍵と利用鍵の組合せでのみオブジェクト鍵を復元可能。

また、次のような工夫により、利用条件の柔軟性と安全性を高めた: (1) 利用/課金条件をコンテンツ単位でなく、オブジェクトと利用法の単位で記述、(2) ACL をコンテンツから分離し、信頼できるチケットサーバに管理を委託。

参考文献

- [1] 細見, 中江, 市山, 「カプセル化コンテンツ流通基盤 (1) - 全体構成と利用状況適応機能 -」, 第57回情報処全国大会, 1998.
- [2] 細見, 谷, 市山, 「多様な再生環境に適応する流通コンテンツ・アーキテクチャの提案」, 第55回情報処全国大会, 1997.

C&C for Human Potential

NEC



じぶん、新しくしたい。

頭のなか、心のなかで生まれたことを、自由に思い通り表現できる。

時間や空間の制約を気にせずに世界中の人々と対話ができる。

好奇心を刺激する情報がどんどん飛び込んでくる…。

デジタルのチカラは、あなたのなかの新しいじぶんが目覚めを促すのを応援します。

さあ、一步前に踏み出して、真新しいじぶんへ。

ちょっとの勇氣とデジタルと。

第57回（平成10年後期）全国大会講演論文集（3）

Copyright© 1998 by The Information Processing Society of Japan

BEST AVAILABLE COPY

平成十年十月五日 発行

編集兼発行 柳 川 隆 之
東京都港区芝浦三 六二〇（芝浦前川ビル7F）

印刷所 三協印刷株式会社
東京都目黒区目黒本町五二〇 七

発行所 社団法人 情報処理学会
東京都港区芝浦三一六二〇（芝浦前川ビル7F）

本論文集に掲載された論文の著作権は（社）情報処理学会に帰属します。

【受入日】 19981016
【情報館受入日】
【CSターム】
【フリーワード】
【許諾レベル】 12
【著者群】
【論文タイトル】 第57回（平成10年後期）全国大会講演論文集（3）
【サブタイトル】 データベースとメディア ネットワーク
【資料タイプ】 学会予稿集
【会議】
【会議名】 第57回（平成10年後期）全国大会
【開催日・発行日】 19981007
第57回会議
【開催場所】 名古屋大学
【主催者】 社団法人情報処理学会 Information Processing Society of Japan
【頁】 1～645